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

Ausgabe 3 / 2020

Krankenhaus-IT JOURNAL

Fakten und Perspektiven der IT im Gesundheitswesen

Covid-19:
Gemeinsam durch die Krise navigieren

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

ENTSCHEIDERFABRIK

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

COVID-19: der digitale Katalysator

Digitale Lösungen in der Gesundheitsversorgung bei COVID-19: Der Markt bietet Lösungen für den Patienten oder den Arzt sowie alle an der Gesundheitsversorgung Beteiligten an. Beispiel telemedizinische Angebote: Sie schützen vor Infektionen, gemeinsam genutzte Plattformen unterstützen den Datenaustausch in Echtzeit und digitale Dokumentationssysteme erleichtern den administrativen Aufwand in Praxis und Krankenhaus.

In der Diskussion um eine Überwindung der COVID-19-Krise geht es darum, die notwendige Patientenversorgung in allen Bereichen wieder sicherzustellen sowie die gesundheitspolitischen Maßnahmen mit Entscheidungen zur Unterstützung der Gesundheitswirtschaft zu verbinden.

So stehen Branchenverbände der Gesundheits-IT medizinischen Einrichtungen bei der Bewältigung der Corona-Krise zur Seite. Kostenlose Angebote stehen zur Verfügung, sie weiten den Support aus. Gleichzeitig fordern sie die Politik auf, Krankenhäuser zu stärken und medizinische Einrichtungen zu entlasten. Das bedeutet auch, das DRG-System anzupassen. Kostensteigerungen, die durch die Corona-Krise in bestimmten Produktbereichen entstanden sind und auch zukünftig relevant sein werden, müssten zusätzlich in der DRG-Kalkulation berücksichtigt werden.

Die Entwicklungen bei COVID-19 offenbaren erheblichen Nachholbedarf in der Digitalisierung der Gesundheitsversorgung. So mussten Einrichtungen ihre Mitarbeiter rasch ins Corona-Home Office schicken. Allerdings legen aktuelle Studienergebnisse nahe, dass die wenigsten IT-Teams auf solche Szenarien vorbereitet sind – mit gravierenden Auswirkungen auf die Sicherheit.

Erfreut sich der Betriebssystem-Oldie Windows 7 nicht einer beträchtlich wachsenden Verbreitung? Grund hierfür ist wohl, dass Angestellte sich ein Home-Office einrichten mussten, und sie reaktivierten hierfür den Desktop- oder Notebook-Rechner, auf dem eben noch Windows 7 läuft.

Die Krise als digitaler Reaktionsbeschleuniger? Allgemein erwartet man, dass der Coronavirus die Implementierung von E-Health vorantreiben wird – vor allem, was telemedizinische und IoT-basierte Gesundheitsüberwachung angeht. Selbst im datenschutzkritischen Deutschland mehren sich die Stimmen der Befürworter.

Herzliche Grüße,
Wolf-Dietrich Lorenz

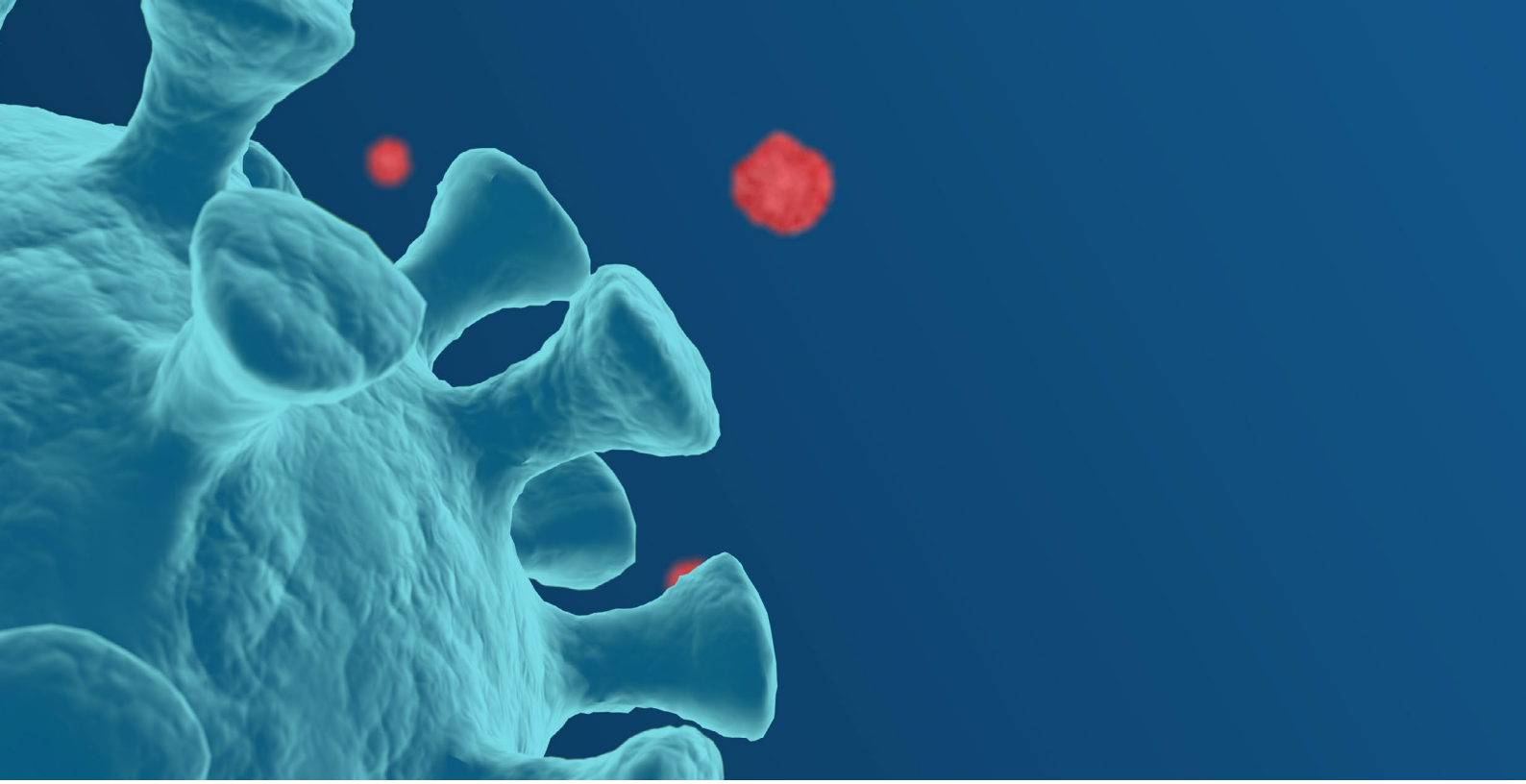
Dagmar Finlayson

Wolf-Dietrich Lorenz

Kim Wehrs

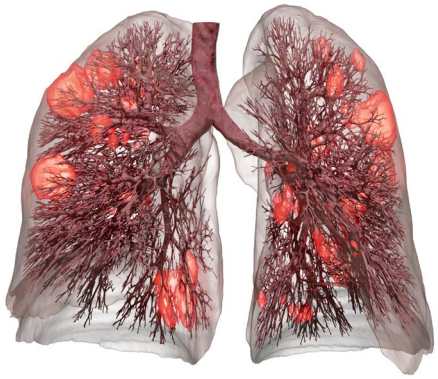
Impressum
Antares Computer Verlag GmbH,
Gießener Straße 4, D-63128 Dietzenbach
E-Mail: antares@medizin-edv.de, www.medizin-edv.de
Verlagsleitung und Herausgeber **Kim Wehrs (kw)**,
stellvertr. **Kai Wehrs (kaw)**. Tel.: 0 60 74/25 35 8, Fax: 0 60 74/2 47 86
Redaktion, Chefredakteurin **Dagmar Finlayson (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
Pixabay S.1,12,16,18,26;
Adobe Stock S.25;
Dedalus Group S.38;
synedra S.43; Ascom S.47;
AD Link S.49;
SHD System-Haus-Dresden GmbH S.58



Titelthema

Verbandsseiten KH-IT



Karriere

Aus dem Markt

IT-Sicherheit im Krankenhaus

Umbruch des Gesundheitssektors und Dynamik der Transaktionen

COVID-19: Gemeinsam durch die Krise navigieren

Die Zahl der Fusionen und Übernahmen ist gegenüber dem Vorjahr noch gewachsen. Die Corona-Krise dürfte die Entwicklung allerdings kurzfristig bremsen. Doch die Digitalisierung des Gesundheitswesens wird die Zahl der Transaktionen steigen lassen.

Die Konsolidierung des deutschen Gesundheitsmarktes setzt sich weiter fort: Für das Jahr 2019 verzeichnet die Branche insgesamt 106 Fusionen und Übernahmen. Im Vergleich zum Vorjahr, das bereits durch ein dynamisches Geschehen geprägt war, ist die Zahl der Transaktionen damit um acht weitere gestiegen. Knapp die Hälfte der Käufe wurden im Bereich der niedergelassenen Leistungserbringer und Labore getätigt, die sich vor allem für Finanzinvestoren zu attraktiven Zielen entwickelten. Das sind zentrale Ergebnisse des „Transaktionsmonitors Gesundheitswesen" der Wirtschaftsprüfungs- und Beratungsgesellschaft PwC.

Michael Burkhart, Leiter des Bereichs Gesundheitswirtschaft bei PwC Germany: „Das deutsche Gesundheitswesen befindet sich in einer Phase des Umbruchs. Stark fragmentierte Märkte – selbst in Ballungsräumen – bieten ein großes Konsolidierungspotenzial. Für Investoren ist der Gesundheitsmarkt so attraktiv, weil er im Vergleich zu anderen Branchen weitgehend unabhängig ist von konjunkturellen Schwankungen. Zudem ist das deutsche Gesundheitswesen von steigenden Patientenzahlen und einer hohen Bonität geprägt."

Die Corona-Krise bremst den Transaktionsmarkt im zweiten Quartal

Allerdings rechnet der Gesundheitsexperte damit, dass die Transaktionen durch die Corona-Krise zumindest kurzfristig zurückgehen dürften und sich auf kleinere Zukäufe etablierter Unternehmen beschränken werden. „Mittelfristig wird sich der Markt jedoch erholen. Diese Entwicklung könnte sich dadurch beschleunigen, dass die Krise gezeigt hat, wie enorm wichtig ein funktionierendes Gesundheitssystem ist", prognostiziert Michael Burkhart. Die Erholung wird auch deshalb schnell gelingen, weil die Organisationen im deutschen Gesundheitswesen ein gutes Krisenmanagement zeigen. „Ich führe das darauf zurück, dass größere Verbünde – etwa im Bereich der Labore – sich schneller und bundesweit einheitlich an die neuen Anforderungen anpassen können", kommentiert der PwC-Gesundheitsexperte.

Auch die Telemedizin dürfte durch die Krise weiter an Bedeutung gewinnen – schon jetzt verzeichnen die Anbieter eine hohe Nachfrage nach Online-Sprechstunden, bedingt durch die Auswirkungen der Pandemie. Obwohl die Digitalisierung des deutschen Gesundheitswesens im Vergleich zu anderen europäischen Ländern noch am Anfang steht, ist davon auszugehen, dass sie enorm an Bedeutung gewinnt und damit auch für eine steigende Zahl an Transaktionen sorgen wird.

Krankenhäuser: Wettbewerb treibt Transaktionsgeschehen

Krankenhäuser und Fachkliniken in Deutschland stehen unter einem hohen Wettbewerbs- und Kostendruck, etwa durch eine Stagnation der Fallzahlen, den Fachkräftemangel im Gesundheitswesen – verschärft noch durch die Einführung der Pflegepersonalgrenze – und den Fixkostendegressionsabschlag. Das führt zu insolvenzgetriebenen Trägerwechseln und strategischen Zusammenschlüssen, insgesamt 26 im Jahr 2019 (2018: 29). Davon sind besonders Krankenhäuser in freigemeinnütziger und teilweise auch in öffentlicher Trägerschaft betroffen. Wichtige Transaktionen waren der Erwerb der Rhön Kliniken durch Asklepios, der Kauf der Caritas Trägergesellschaft West durch die Josefs-Gesellschaft und den Caritasverband des Bistums Aachen sowie die Veräußerung der DRK Kliniken Berlin Brandenburg an die KMG Kliniken im Zuge eines Insolvenzverfahrens.

Durch die Corona-Krise navigieren die Krankenhäuser derzeit souverän. "In der Krise zeigt sich, dass die Häuser durch

die Trägervielfalt in der Lage sind, entsprechend ihrer spezifischen Stärken zu reagieren - etwa durch Kooperationen und effiziente Strukturen. Diese Vielfalt sollten wir erhalten und nicht zugunsten einer stärkeren Verstaatlichung aufgeben", sagt Michael Burkhart.

Rehabilitation: Der ambulante Markt zieht Investoren an

Auf dem Transaktionsmarkt spielt der Bereich Rehabilitation mit sieben Übernahmen nur eine untergeordnete Rolle (2018: 6). Gerade die ambulante Rehabilitation hat in den vergangenen Jahren aber durch steigende Fallzahlen an Bedeutung gewonnen. An diesem Markt zeigen sowohl Finanzinvestoren als auch strategische Investoren vermehrt Interesse. Im Bereich der stationären Rehabilitation wird die Konsolidierung voraussichtlich durch das anstehende Intensivpflege- und Rehabilitationsstärkungsgesetz weiter zunehmen. Wesentliche Transaktionen im Segment Pflege waren der Erwerb der Kliniken Wied durch die Median-Kliniken, der Kauf der Rehaklinik Masserberg durch die Regiomed-Kliniken und der Erwerb von Rehacon durch Waterland.

Michael Burkhart, Leiter des Bereichs Gesundheitswirtschaft bei PwC Germany

Abhängigkeit von Technologien und Wirtschaftsprozessen

Corona-Pandemie: Gesellschaftliche und technische Folgen der Krise

Die Coronakrise hat Deutschland fest im Griff. Das Abstandhalten oder Social Distancing prägt unseren Alltag, privat wie beruflich. Digitale Technologien sind dabei eine große Hilfe, können analoge Kommunikation auf Dauer aber nicht ersetzen, sagt Physiker und Philosoph Armin Grunwald, Experte für Technikfolgenabschätzung am Karlsruher Institut für Technologie (KIT) im Interview.

Digitale Kommunikationstechnologien unterstützen uns derzeit dabei, die Folgen der Krise abzufedern. Kann die Technik auch helfen, noch größere ökonomische und gesellschaftliche Verwerfungen zu verhindern?

Armin Grunwald: Die Digitalisierung hilft sehr, in der Krise vieles aufrechtzuerhalten, was analog zurzeit nicht geht: vom Homeoffice mit Videokonferenzen bis zum Schulunterricht oder universitären Lehrbetrieb von zu Hause aus. Allerdings ist Technik nicht alles. Sie macht den Verlust von Gemeinschaft und die soziale Isolierung für eine gewisse Zeit zwar leichter erträglich, bleibt aber doch nur ein Ersatz für echte menschliche Begegnung. Für manche Zwecke wie organisatorische Besprechungen ist sie ein sehr guter, für andere wie Gottesdienste oder Live-Konzerte eher ein fader Ersatz.

Wird sich unser Arbeitsleben auch über die Krise hinaus dauerhaft verändern?

Grunwald: Wir lernen unter dem aktuellen Zwang viel schneller, mit den digitalen Werkzeugen umzugehen. Wir lernen, analoge und digitale Formate in ihren jeweiligen Vor- und Nachteilen viel besser einzuschätzen. Das gilt für digitalen Unterricht genauso wie für berufliche Dinge oder auch private Kommunikation. Ich denke schon, dass wir mit dieser neu erworbenen oder stark vertieften Kompetenz bessere Kombinationen von analog und digital im Arbeitsleben auch auf Dauer behalten werden. Aber: Gerade komplexe inhaltliche Diskussionen funktionieren in der digitalen Ersatzkommunikation eher schlecht. So lebt unter anderem die Wissenschaft vom inhaltlichen Dialog, vom lebendigen Austausch, vom Brainstorming, von neuen Konstellationen, vom Streit um das beste Argument.

Neben dem Social Distancing werden auch technische Lösungen diskutiert, um die Pandemie einzudämmen, beispielsweise die Erhebung von Bewegungsprofilen. Welche unerwünschten Folgen müssen wir bei ihrem Einsatz im Auge behalten?

Grunwald: Totalkontrolle wäre aus Sicht mancher Wissenschaftler und Politiker eine schöne technische Lösung zur Überwachung und Isolierung, zum Beispiel auch von Gefährdern und Gefährdeten. Dann könnten die anderen weitgehend normal weiterleben. Dahinter stehen komplexe Abwägungen, für die es nicht einfach eine Bewertung nach richtig oder falsch gibt. Ich halte solche Überlegungen in Notstandszeiten – auch wenn wir dieses Wort nicht verwenden sollen – für legitim, wenn die Maßnahmen hart zweckgebunden und auf ein Minimum beschränkt werden, sowie ihre Durchführung streng überwacht wird. Das können mögliche Übergangslösungen sein, sobald das Social Distancing gelockert wird, um ein Wiederaufflackern der Virusausbreitung zu verhindern.

Die aktuellen politischen und gesellschaftlichen Kraftanstrengungen sind enorm: Ein Vorbild für die Bewältigung anderer globaler Herausforderungen wie der Klimakrise?

Grunwald: Die Coronakrise verringert die Umweltverschmutzung, die Wirtschaft runterzufahren, nützt dem Klima. Aber das ist nun wirklich keine Lösung! Ich befürchte, dass das gerade wieder erwachte Problembewusstsein zum Klimawandel erstmal weg ist. Auch einflussreiche Zeitungen schreiben schon, dass angesichts des Virus das Klima vielleicht doch nur ein Scheinproblem sei. Das ist gefährlich, denn das Klimaproblem bleibt und wird sich verschärfen.

Welche Schlüsse sollten wir aus der derzeitigen Situation ziehen? Muss Technologieentwicklung künftig verstärkt auf ihre Resilienz in Krisensituationen ausgerichtet sein?

Grunwald: Unbedingt müssen wir uns unsere krasse Abhängigkeit von Technologien und Wirtschaftsprozessen stärker ins Gedächtnis rufen. Ohne Strom und Internet, ohne globale Lieferketten und Mobilität bricht alles zusammen. Wir haben uns zu sehr daran gewöhnt, dass immer alles funktioniert. Ist ja auch bequem. So wurden auch Studien zu möglichen Virusepidemien weitgehend ignoriert. Wir brauchen viel stärker ein Bewusstsein, dass auch alles anders laufen könnte, auch wenn das unbequem ist und die abendliche Gemütlichkeit auf dem Sofa stört. Wir brauchen Pläne B für den Fall der Fälle. Und wir brauchen Technologien, die nicht alles auf eine Karte setzen. Das kann für Dezentralisierung sprechen, zum Beispiel in der Energiewende oder im Digitalbereich.

Die Expertise von Wissenschaftlerinnen und Wissenschaftlern hat derzeit einen hohen Stellenwert in der Bevölkerung und großen Einfluss auf politische Entscheidungen. Stehen wir vor grundsätzlichen Veränderungen bei der wissenschaftlichen Beratung von Politik und Gesellschaft?

Grunwald: An der Schnittstelle zwischen Politik und Gesellschaft laufen seit Jahrzehnten Veränderungen. Wissenschaft ist gefragt, steht aber auch unter Legitimationsdruck. Daran ändert die Krise nichts. Wissenschaft steht vielleicht noch ein wenig stärker in der gesellschaftlichen Verantwortung als zuvor. Aber da gehört sie auch hin, und das nicht nur als Virologie, sondern übergreifend.

Armin Grunwald ist Physiker und Philosoph. Am KIT leitet er das Institut für Technikfolgenabschätzung und Systemanalyse (ITAS). Als Leiter des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) in Berlin ist er seit vielen Jahren in der Politikberatung aktiv.

Künstliche Intelligenz hilft bei der Interpretation

Computermodell ermöglicht schonende Beatmung bei Corona

Eine künstliche Beatmung kann Leben retten, nicht nur bei schweren Verläufen einer Covid-19-Erkrankung. Gleichzeitig ist die Druckbeatmung aber auch eine extreme Belastung für das Lungengewebe. Besonders bei vorgeschädigter Lunge kann dies tödliche Folgen haben. Ein digitales Modell der Lunge wurde an der Technischen Universität München (TUM) entwickelt. Es ermöglicht eine schonendere Beatmung und könnte so die Zahl der Todesfälle bei Covid-19 und ARDS deutlich reduzieren und die Überlebenschancen erhöhen.

Lunge mit Covid-19: Aus den Daten eines Computer-Tomogramms kann das Programm mithilfe künstlicher Intelligenz den aktuellen Zustand der Patientenlunge berechnen. Das Bild zeigt eine durch eine Covid-19-Infektion (orange Bereiche) geschädigte Lunge.
Bild: Jakob Richter / Ebenbuild / TUM

Für Patienteninnen und Patienten mit akutem Lungenversagen (Acute Respiratory Distress Syndrome, ARDS) ist die künstliche Beatmung die Rettung. Doch die Situation ist paradox: Während die Mediziner versuchen, mit Druck die Lunge offen zu halten und den Austausch von Sauerstoff und Kohlendioxid weiter zu ermöglichen, kann der Druck Teile der Lunge auch so stark schädigen, dass dies tödliche Folgen hat. Den behandelnden Medizinern stehen nur wenige Parameter zur Verfügung, um die optimale Beatmung einzustellen. Doch die Lunge ist ein komplexes Organ. Der Druck, der benötigt wird, um alle Bereiche offen zu halten, kann in manchen Bereichen schon zu Überdehnungen führen. Gleichzeitig muss ein wiederholtes Öffnen und Schließen einzelner Lungenbereiche vermieden werden. Denn das Gewebe reagiert auf den mechanischen Reiz in beiden Fällen mit einer Entzündung.

Unsichtbares sichtbar machen

„Die Krux dabei ist", sagt Wolfgang Wall, Professor für Numerische Mechanik an der TU München, „dass die Behandelnden bisher keine Möglichkeit hatten, eine Überdehnung zu erkennen. Von der Luftröhre bis in die feinsten Verästelungen besitzt die Lunge mehr als 20 Stufen der Verzweigung, und es gibt keine Messmethode um festzustellen, was auf der Mikroebene der Lunge während der Beatmung passiert." Die Lunge ist im Bereich der „Lungenbläschen", die in vielen Fachbüchern noch immer fälschlicherweise wie Weinreben dargestellt werden, in Wahrheit ein schwammartiges Gewebe über dessen feinste Wände der Austausch zwischen der Luft und dem Blut erfolgt. Die mechanischen Wechselwirkungen zwischen den verschiedenen Gewebearten, der strömenden Luft und dem Flüssigkeitsfilm auf dem Gewebe sind extrem komplex.

Viele Jahre Forschung mit immer weiter verfeinerten Simulationsmodellen für das Verhalten von Gewebe und Luftstrom sowie mit mikromechanischen Versuchen an realen Gewebeproben haben nun zu einem digitalen Lungenmodell geführt. Ausgehend von den Daten eines Computer-Tomogramms des Brustkorbs und der Analyse eines Atemzuges zeigt es dem Behandelnden, welche Einstellungen des Beatmungsgeräts zu welchen Belastungen auf der Mikroebene der Lunge führen. Entsprechend kann dieser die Einstellungen anpassen.

Künstliche Intelligenz hilft bei der Interpretation

Klinischer Standard ist es, die Einstellungen für die Beatmung anhand einer vom Körpergewicht ausgehenden Faustformel zu berechnen. Aus den Daten eines Computer-Tomogramms errechnet das Computermodell der Arbeitsgruppe von Prof. Wall das tatsächliche Lungenvolumen. Es erkennt dabei sogar den Zustand einzelner Lungenbereiche, die durch die Erkrankung bereits geschädigt sind.

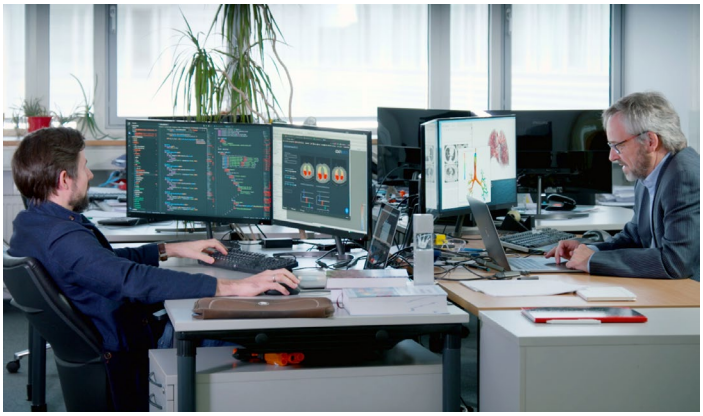
Aus der Druck- und Volumenänderung während eines Atemzuges errechnet der Computer dann Werte für die mechanischen Eigenschaften der Lunge des Patienten. Damit erzeugt das Modell einen digitalen Zwilling der Patientenlunge. Er ist so präzise, dass das Programm voraussagen kann, welche Einstellungen zu Schäden führen würden.

Automatische Modellerstellung mittels künstlicher Intelligenz

Parallel zur weiteren Forschung zusammen mit klinischen Partnern gründete Prof. Wall zusammen mit drei ehemaligen Mitarbeitern das Unternehmen „Ebenbuild", um die Forschungsergebnisse schnellstmöglich in die klinische Praxis zu bringen. Ein wesentlicher Schritt dabei war die automatische Modellerstellung mittels künstlicher Intelligenz. Auf dieser Basis wurde inzwischen auch ein Werkzeug zur Charakterisierung der Lunge entwickelt, das auch zur frühen Erkennung von Covid-19 eingesetzt werden kann.

„Über 80 Prozent der Todesfälle infolge von Covid-19 sind auf akutes Lungenversagen zurück zu führen. Bei längerfristiger künstlicher Beatmung von Patienten sinkt die Überlebensrate derzeit auf etwa 50 Prozent", sagt Prof. Wall. „Ziel unserer Arbeiten ist es, dass in Zukunft an jedem Beatmungsplatz ein digitales Lungenmodell bei der optimalen Einstellung der Beatmung hilft und wir so die Überlebenschance deutlich erhöhen können."

Die Forschungsarbeiten wurden von der Deutschen Forschungsgemeinschaft gefördert. Die Ausgründung „Ebenbuild" wird im Rahmen des EXIST-Programms aus Mitteln des Bundeswirtschaftsministeriums gefördert. Grundlegende Modellrechnungen wurden am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften auf dem Campus Garching durchgeführt.



Arbeit am Lungenmodell: Prof. Wall und Dr. Biehler arbeiten an der weiteren Verfeinerung ihres digitalen Lungenmodells.
Bild: Andreas Kerler / bavariaone / TUM

Publikationen

C. J. Roth, T. Becher, I. Frerichs, N. Weiler, W. A. Wall:
Coupling of EIT with computational lung modelling for predicting patient-specific ventilatory responses
Journal of Applied Physiology, 122 (2017), 855-867 – DOI: 10.1152/japplphysiol.00236.2016

C. J. Roth, M. Ismail, L. Yoshihara, W. A. Wall:
A comprehensive computational lung model incorporating inter-acinar dependencies: Application to spontaneous breathing and mechanical ventilation
International Journal for Numerical Methods in Biomedical Engineering, 33 (2017), e02787
DOI: 10.1002/cnm.2787

C. J. Roth, L. Yoshihara, W. A. Wall:
Computational Modeling of Respiratory Biomechanics
In R. Narayan (Ed.), Encyclopedia of Biomedical Engineering, Elsevier, 2018, vol. 2, pp. 70–80

Hersteller durch Produkthaftung in die Verantwortung nehmen

KI für die Medizin: Patientendaten nutzen und schützen

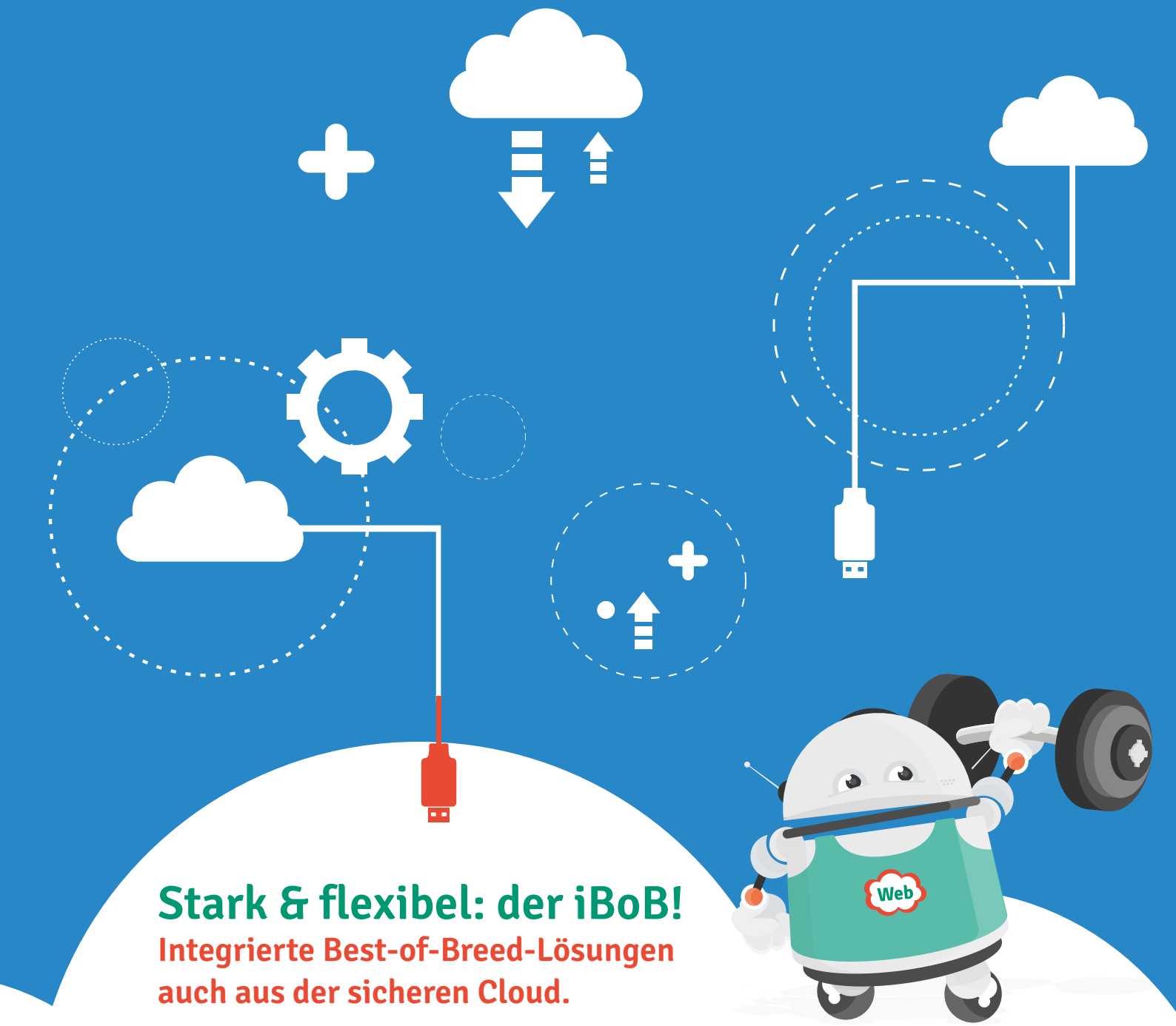
Der Einsatz von Künstlicher Intelligenz (KI) in der Medizin verspricht großen Nutzen für Patientinnen und Patienten. KI-basierte Assistenzsysteme unterstützen das frühe Erkennen von Krankheiten, ermöglichen ein schnelles Auswerten großer Mengen von Bild- und Labordaten und bieten die Chance für individuelle Therapien. Mit einer verbesserten Gesundheitsversorgung mit Hilfe von KI und den damit verbundenen Herausforderungen für die IT-Sicherheit befasst sich das Karlsruher Institut für Technologie.

Der Einsatz von Künstlicher Intelligenz (KI) verspricht in der Medizin große Verbesserun-gen. Lernende Systeme können künftig bei der Prävention, frühzeitigen Diagnose sowie der patientengerechten Therapie zu besseren Behandlungsergebnissen führen und somit unsere Gesundheitsfürsorge verbessern. Durch die Nutzung von patientenindividuellen medizinischen Daten und KI-Assistenzsystemen lassen sich künftig neue medizinische Zusammenhänge entdecken, innovative Präventionsansätze entwickeln, schneller Diagnosen stellen und seltene Erkrankungen früher erkennen. Der Einsatz von KI-Systemen kann zudem Ärztinnen und Ärzte sowie medizinisches Pflegepersonal bei einer verbesserten Versorgung von Patientinnen und Patienten unterstützen und das medizinische Personal entlasten.

Zudem ermöglichen KI-basierte medizinische Systeme differenziertere Behandlungsmethoden sowie bessere Ergebnisse in der Vor- und Nachsorge. Gleichzeitig stellt der Einsatz von intelligenten und selbstlernenden Systemen im Gesundheitswesen hohe Anforderungen an die IT-Sicherheit der Systeme. Risiken des Einsatzes von KI-Systemen im Gesundheitswesen sind zu identifizieren und mögliche Lösungsvorschläge dafür aufzuzeigen. Nur so kann Vertrauen in die Sicherheit von KI-unterstützten medizinischen Systemen geschaffen werden, was als Voraussetzung für dessen Nutzung gilt. Mögliche Risiken beim Einsatz Lernender Systeme im Gesundheitsbereich sind fehlerhafte oder bewusst verfälschte Trainingsdaten, Angriffe auf die KI-Software,Verletzungen der Privatsphäre der Patientinnen und Patienten sowie Angriffe auf KI-Datenbanken und die fehlende Integration in die klinische Praxis.

KI-basierte Assistenzsysteme unterstützen das frühe Erkennen von Krankheiten, ermöglichen ein schnelles Auswerten großer Mengen von Bild- und Labordaten und bieten die Chance für individuelle Therapien. Mit einer verbesserten Gesundheitsversorgung mit Hilfe von KI und den damit verbundenen Herausforderungen für die IT-Sicherheit befasst sich das aktuelle Whitepaper „Sichere KI-Systeme für die Medizin“. Veröffentlicht hat es die vom Bundesministerium für Bildung und Forschung initiierte Plattform Lernende Systeme (PLS), in der verschiedene Arbeitsgruppen zeigen, wie KI im Sinne von Mensch und Gesellschaft gestaltet werden kann. Jörn Müller-Quade, Professor für Kryptographie und Sicherheit am KIT, ist einer der Autoren des Whitepapers. Er leitet, gemeinsam mit der an der Universität Tübingen lehrenden Philosophin Jessica Heesen, die interdisziplinär besetzte Arbeitsgruppe IT-Sicherheit, Privacy, Recht und Ethik der PLS.

„KI-Systeme brauchen große Datenmengen, damit sie aus ihnen lernen können. Die Herausforderung besteht darin, die Patientendaten sowohl zu nutzen als auch sie zu schützen“,



Stark & flexibel: der iBoB!

Integrierte Best-of-Breed-Lösungen auch aus der sicheren Cloud.

Mit der Lösungsfamilie für Verwaltung, Medizin, Pflege, Ambulanz und MVZ bietet Ihnen UWS das, woran sich die Monolithen derzeit die Zähne ausbeißen: mobile, Cloud-orientierte, nutzerorientierte Fachanwendungen.

Um fit zu sein für den digitalen Wandel und die geforderte Vernetzung, müssen sich die Krankenhäuser jetzt neu aufstellen. Anwendungen und Infrastruktur sind hierbei die wesentlichen Komponenten. Mit dem KIS CLINIXX®, das mit den leistungsstarken Lösungen der UWS-Mitgliedsunternehmen integriert ist, lassen sich die Prozesse in allen Krankenhausbereichen sicher und zügig digitalisieren.

Auf dieser Basis macht der digitale Wandel Spaß!

UWS-Mitgliedsunternehmen:

- AMC, Hamburg
- apenio, Bremen
- blueAlpha, Zweibrücken
- ID, Berlin
- docuvita, Bad Soden
- Imilia, Berlin
- LOWTeq, Köln
- medatixx, Eltville am Rhein
- SIEDA, Kaiserslautern
- Transact, Hamburg

www.unitedwebsolutions.de

United Web Solutions for Healthcare

sagt Müller-Quade. Durch die Vielzahl der Akteure im Gesundheitswesen haben viele Personen potenziell Zugriff auf die Patientendaten. „Dies macht es schwierig, sensible Gesundheitsdaten vor unberechtigtem Zugriff zu schützen", so der Kryptograph. Es gebe informationstechnologische Lösungen für die sichere Datenübertragen und die Zugangskontrolle, „wenn aber die Endgeräte, der PC der Apotheke, der Krankenversicherung oder des Mediziners, nicht sicher sind, werden wir Probleme haben, die zu Datenskandalen führen könnten", sagt Müller-Quade, der am KIT die Forschungsgruppe Kryptographie und Sicherheit leitet und Initiator des Kompetenzzentrums für IT-Sicherheit KASTEL am KIT ist. „Wichtig wäre eine Produkthaftung, damit Hersteller sich in der Verantwortung sehen, sicherere Produkte zu entwickeln."

KI-Systeme im Betrieb ohne menschliche Überwachung

Für ebenfalls notwendig hält er die Zertifizierung von KI-Systemen und -Datenbanken in der Medizin sowie der elektronischen Patientenakte (ePA) durch unabhängige Prüfstellen. Eine besondere Herausforderung sieht der Informatiker im Einsatz kontinuierlich weiter lernender KI-Systeme, deren Software sich im Betrieb ohne menschliche Überwachung verändert. Die Entscheidungen eines solchen ein KI-Systems sollten durch die behandelnden Menschen daraufhin überprüft werden, ob sie nachvollziehbar sind. Hier würde eine erklärbare KI enorm helfen, so der Wissenschaftler. „Ärztinnen und Ärzte dürfen das vorgeschlagene Ergebnis nicht unreflektiert übernehmen."

„Wenn wir intelligente IT in der Medizin nutzen wollen, werden Datenskandale, obwohl sehr auf Sicherheit geachtet wird, voraussichtlich nicht ausbleiben", befürchtet Müller-Quade. Ihre Auswirkungen ließen sich aber einschränken, wenn Gesundheitsdaten aus Datenlecks nicht zum Nachteil der Patienten genutzt werden dürften. Es gelte Diskriminierung aufgrund von Kenntnissen aus solchen Datenlecks zu verhindern, etwa wenn jemand aufgrund von bekannt gewordenen Vorerkrankungen eine Arbeitsstelle nicht bekommt. „Es wäre wichtig, künftig auf technischer Ebene nachweisen zu können, dass ein Algorithmus diskriminierungsfrei entscheidet."

Grundregeln der IT-Sicherheit einhalten

Mit der geplanten Einführung der ePA erhalten Patientinnen und Patienten die volle Kontrolle über ihre Gesundheitsdaten, die dann auch auf dem eigenen PC gespeichert sind. Umso mehr gelte es, bestimmte Grundregeln der IT-Sicherheit einzuhalten – immer das neueste Betriebssystem zu nutzen und sichere Passwörter zu verwenden –, andernfalls könne der PC zum Einfallstor für Angreifer werden und die Krankengeschichte offenliegen.

Die Veröffentlichung „Sichere KI-Systeme für die Medizin – Whitepaper aus der Plattform Lernende Systeme" (1) eranschaulicht in einem fiktiven Anwendungsszenario „Mit KI gegen Krebs" den möglichen Einsatz von KI am Beispiel eines Lungenkrebspatienten. Sie wendet sich an politische Entscheiderinnen und Entscheider und bietet darüber hinaus allen Interessierten Einblick in das Thema Datenmanagement und IT-Sicherheit in der Medizin.

(1) Jörn Müller-Quade et al. (Hrsg.): Sichere KI-Systeme für die Medizin – Whitepaper aus der Plattform Lernende Systeme, München 2020. Das Whitepaper steht zum Download bereit unter: https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_6_Whitepaper_07042020.pdf

Plattform Lernende Systeme

Systeme im Sinne der Gesellschaft zu gestalten – mit diesem Anspruch wurde die Plattform Lernende Systeme im Jahr 2017 vom Bundesministerium für Bildung und Forschung (BMBF) auf Anregung des Fachforums Autonome Systeme des Hightech- Forums und acatech – Deutsche Akademie der Technikwissenschaften initiiert. Die Plattform bündelt die vorhandene Expertise im Bereich Künstliche Intelligenz und unterstützt den weiteren Weg Deutschlands zu einem international führenden Technologieanbieter. Die rund 200 Mitglieder der Plattform sind in Arbeitsgruppen und einem Lenkungskreis organisiert. Sie zeigen den persönlichen, gesellschaftlichen und wirtschaftlichen Nutzen von Lernenden Systemen auf und benennen Herausforderungen und Gestaltungsoptionen

Jörn Müller-Quade, Professor für Kryptographie und Sicherheit am KIT: „Wenn wir intelligente IT in der Medizin nutzen wollen, werden Datenskandale, obwohl sehr auf Sicherheit geachtet wird, voraussichtlich nicht ausbleiben."

Soft Privacy Technologies‘ als Option

Datenschutz bei Corona-Tracing-Apps

Tracing-Apps sollen dabei helfen, die Ausbreitung des Coronavirus einzudämmen: Ist jemand erkrankt, lassen sich dank der Apps Kontaktpersonen nachvollziehen und warnen. Wie sicher sind die Nutzerdaten mit zentralen oder mit dezentralen Lösungen? Die deutsche Bundesregierung hat sich auf ein System verständigt, das Daten dezentral speichert. Professor Thorsten Strufe, Leiter der Forschungsgruppe „Praktische IT-Sicherheit“ am Karlsruhe Institut für Technologie (KIT), und sein Team haben beide Ansätze einander gegenübergestellt und untersucht, wie datenschutzkonform sie wirklich sind.

„Der Unterschied der beiden Ansätze liegt lediglich darin, ob das Prüfen von Kontakten mit Erkrankten dezentral auf den Mobilgeräten oder zentral auf einem Server stattfindet“, erläutert Strufe. Befürworter der dezentralen Lösung argumentierten: Werde ein Nutzer, der nur eine andere Person getroffen hat, anschließend über eine potenzielle Infektion informiert, wisse er ohnehin, wer die infizierte Person sei. Ein zentraler Server hingegen, der die Kontakte zwischen allen positiv Getesteten und potenziell Infizierten berechnet, könne im Zweifel die Informationen aller Benutzer auswerten. „Der Verlust der Privatheit aller Daten gegenüber einem zentralen Betreiber wird also als viel schwerwiegender eingeschätzt als der Verlust der Privatheit Einzelner gegenüber ihren Kontakten“, so Strufe, der Professor für praktische IT-Sicherheit ist. „Unsere Untersuchungen zeigen aber, dass keine der bislang insgesamt diskutierten Lösungen wirklich umfassend die Daten der Nutzerinnen und Nutzer schützt. Keiner der beiden Ansätze, zentral oder dezentral, ist dem anderen grundsätzlich überlegen – für beide kann es aber Lösungen geben, die vollkommen identische Schutzeigenschaften haben.“ Hier gelte es nun, intensiv an der Weiterentwicklung zu arbeiten.

Strufe und sein Team haben untersucht, wie datenschutzkonform verschiedene bisherige Vorschläge sind. Zwar erhoben viele den Anspruch, die Privatsphäre zu wahren, keinem sei dies bislang aber vollständig gelungen. „Zwar schließen die meisten Vorschläge gewisse mögliche Datenlücken aus, lassen dabei allerdings andere außer Acht“, so Strufe.

Die Wissenschaftlerinnen und Wissenschaftler haben zunächst den Begriff der Privatsphäre modelliert, um anhand dessen die verschiedenen App-Ansätze zu untersuchen. „Eins ist klar: Gewisse Informationen muss die App sammeln – beispielsweise wer wann andere Personen für wie lange trifft“, sagt Strufe. Dabei gelte es aber zu verhindern, dass Gesundheitszustände, Aufenthaltsorte, soziale Interaktionen oder Gewohnheiten der Personen an neugierige Benutzer, Dienstanbieter oder externe Dritte durchsickern.

Trotzdem sieht er die Tracing-App unter bestimmten Voraussetzungen als Option: „Zum einen wäre ein System mit ‚Soft Privacy Technologies‘ denkbar, bei dem wir einer Instanz wie dem Robert Koch-Institut über verschlüsselte Kanäle die Daten spenden und darauf vertrauen, dass diese dort zu exakt dem Zweck des Contact-Tracings und zu nichts anderem genutzt werden.“ Dies setze natürlich eine Freiwilligkeit und eine klare, verständliche Einwilligung der Nutzerinnen und Nutzer voraus.

„Zum anderen müssten die App-Entwickler einen Schritt zurückgehen. Bisher hat man den Eindruck, dass es ein Wettlauf unterschiedlicher Initiativen war. Es wäre aber besser, zunächst die notwendige Funktion zu verstehen, die potenziellen Bedrohungen klar zu benennen und anschließend gemeinsam ein umfassend sicheres System zu entwickeln.“ Dabei gelte es darauf zu achten, dass keine großen Firmen als Treuhänder der Daten auftreten.

Formale Definitionen – wie sie Strufe und sein Team unter anderem für den Begriff „Privatsphäre“ aufgestellt haben – erleichterten nicht nur eine systematische Sicherheitsanalyse, sondern machten es auch möglich, verschiedene App-Vorschläge im Hinblick auf den Schutz zu vergleichen, den sie bieten. Dies schaffe die Grundlage für den Entwurf datenschutzfreundlicherer Anwendungen.

Weitere Information

Covid Notions: Towards Formal Definitions – and Documented Understanding – of Privacy Goals and Claimed Protection in Proximity-Tracing Services
https://arxiv.org/pdf/2004.07723.pdf

Professor Thorsten Strufe, Leiter der Forschungsgruppe „Praktische IT-Sicherheit“ am Karlsruhe Institut für Technologie (KIT)

Offener Brief: Geplante Corona-App ist höchst problematisch

Gemeinsam mit anderen Vereinen richtet die Gesellschaft für Informatik einen offenen Brief an die Bundesminister Jens Spahn und Helge Braun zur möglichen Apps zur Kontaktverfolgung. Es geht um eine Corona-Tracing-App auf Basis des Softwaregerüsts der Initiative PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) mit zentralem Matching.

Sehr geehrter Herr Bundesminister Spahn, sehr geehrter Herr Kanzleramtsminister Braun, wie Medienberichten zu entnehmen ist, plant das Bundesgesundheitsministerium nun mit einer Corona-Tracing-App auf Basis des Softwaregerüsts der Initiative PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) mit zentralem Matching.

Diese Entscheidung stößt bei uns zwischenzeitlich auf großes Unverständnis, da gerade dies der problematischste unter den vorliegenden Entwürfen ist. Nachdem PEPP-PT nicht in der Lage war, schnell eine halbwegs funktionierende und datenschutzfreundliche Lösung zu liefern, sollte nun den technisch ausgereiften und datenschutzrechtlich gebotenen Ansätzen unbedingt der Vorzug gegeben werden. In der derzeitigen politischen Diskussion werden Erwartungen für eine Corona-Tracing-App geschürt, die möglicherweise nicht eingehalten werden können. Inwiefern sie die Pandemie-Bekämpfung unterstützen kann, wird erst in Monaten zu beurteilen sein. Wir bitten aus diesen Gründen darum, eine Neubewertung der verschiedenen Optionen zu vollziehen und dabei die Argumente und Vorbehalte vieler Expertinnen und Experten stärker zu berücksichtigen sowie ausschließlich auf Lösungen zu setzen, die – im Gegensatz zu dem vorliegenden Vorschlag – technisch von den Betriebssystem- Anbietern auch umsetzbar sind. Eine Corona-Tracing-App sollte, wenn überhaupt, nur auf Basis eines dezentralen Ansatzes – wie beispielsweise das Konzept DP- 3T (Decentralized Privacy Preserving Proximity Tracing) – aufgebaut und programmiert werden. Andernfalls steht zu befürchten, dass der geringe Datenschutz eines zentralen Ansatzes und das Fehlen technischer Beschränkungen gegen Zweckentfremdung dazu führen wird, das Vertrauen in die Verwendung einer solchen App auszuhöhlen und damit die Akzeptanz für spätere digitale Lösungen leichtfertig zu unterminieren.

In der Tat können digitale Lösungen in vielen Fällen maßgeblich dabei helfen, Probleme zu identifizieren und zu lösen – auch bei der Bekämpfung der Pandemie haben digitale Lösungen durchaus ihren Platz. Das haben zivilgesellschaftliche Projekte wie der #WirVsVirus-Hackathon gezeigt. Doch die am Mittwoch veröffentlichten Pläne des Bundesgesundheitsministeriums sind nur eine scheinbar sinnvolle Verwendung digitaler Lösungen im Kampf gegen die Ausbreitung des Corona-Virus. In Wahrheit sind sie für unsere freiheitlich-demokratische Gesellschaft hochproblematisch und ignorieren die Fachdebatte.

Rund 300 internationale Wissenschaftlerinnen und Wissenschaftler haben diese Woche einen offenen Brief unter-

zeichnet, in dem sie das Datenschutzkonzept von PEPP-PT aufgrund des zentralen Datenspeicherungsansatzes deutlich kritisieren und davon abraten. Zwar wird die zentrale Speicherung unter Datenschutzaspekten damit verteidigt, dass die Daten pseudonymisiert werden. Eine Zurückverfolgung und De-Anonymisierung etwa von infizierten Personen ist bei der Datenerhebung jedoch mit deutlich geringerem Aufwand als bei einem dezentralen Ansatz möglich, wenn die versendeten IDs auf Personen zurückführbar sind. Jedem Ansatz eines möglichen Missbrauchs von Gesundheitsdaten muss entschieden entgegengetreten werden.

Die Europäische Union hat derzeit weltweit ein Alleinstellungsmerkmal mit hohen Datenschutzanforderungen und der auch international wegweisenden Datenschutzgrundverordnung (DSGVO). Durch Forderungen – unter anderem der deutschen Regierung –, Datenschutzanliegen im Angesicht der Pandemie hintanzustellen, werden Glaubwürdigkeit und Gestaltungswirkung für die Zukunft verspielt. Zudem ist ein gemeinschaftlicher europäischer Ansatz bei der Bekämpfung des Virus und für die Kontaktnachverfolgung im gemeinsamen europäischen Binnenmarkt essentiell.

Uns besorgen zudem die immer lauter werdenden Rufe nach einer „Pflicht zur App" für gewisse Bereiche des Lebens. Die gemeinsame Bekämpfung der Pandemie benötigt Vertrauen und die Kooperation aller. Die Bereitschaft dazu wird mit einer Pflicht ohne Not verspielt. Eine allgemeine Bürgerpflicht, die jede Bürgerin und jeden Bürger zur Preisgabe sensibler Informationen verpflichtet, ist mit einem freiheitlichen Staat nicht zu vereinbaren. Auch die Einführung einer indirekten App-Pflicht, die das Betreten bestimmter Orte von ihrer Verwendung abhängig machen würde, lehnen wir ausdrücklich ab.

Dass es auch anders geht, zeigen die Schweiz und Österreich. Dort wurden Empfehlungen von Expert*innengruppen berücksichtigt, und die Regierungen setzen auf dezentrale und transparente Konzepte. Dabei handelt es sich um exakt den Ansatz, für den sich die beiden Marktführer für Smartphone-Betriebssysteme, Google und Apple, bereits zur Kooperation bereit erklärt haben. Dies ist eine Bedingung, die für den Erfolg einer App immanent ist, denn ohne die Zusammenarbeit mit den beiden Unternehmen, die fast 100 Prozent des Smartphone-Marktes abdecken, ist ein Scheitern der Tracing-App vorhersehbar. Denn der hier gewünschte Einsatzzweck der Bluetooth-Technologie ist neu und in diesem Ausmaß gänzlich unerprobt. Ob die Technologie verlässliche Ergebnisse liefern kann, ist umstritten. Es ist daher unabdingbar, die Betriebssystemhersteller mit einzubeziehen, um eine realistische Chance für einen neuen Einsatzzweck der Technologie zu ermöglichen.

Eine App, die zumindest eine Aussicht auf Erfolg haben soll, muss ein transparentes Konzept verfolgen, quelloffen programmiert werden, auf zentrale Datenspeicherung verzichten und die Anonymität der Nutzerinnen und Nutzer so weitgehend wie möglich schützen. Diese Anforderungen erfüllt der nun eingeschlagene Weg nicht.

Sehr geehrter Herr Bundesminister Spahn, sehr geehrter Herr Kanzleramtsminister Braun, als Unterzeichnende bitten wir Sie deshalb, die Forderungen aus der Wissenschaft und die Bedenken der IT-Expertinnen und -Experten ernstzunehmen und nicht auf einen Weg zu bauen, der von vornherein absehbar zu deutlichen Akzeptanzproblemen führen wird. Das von Ihnen präferierte Konzept für die App ist nicht der richtige Weg. So wird der Gedanke einer digitalen Lösung zur Bruchlandung – und das kann sich in der Bekämpfung der Pandemie niemand leisten.

Unterzeichnende:

D64 – Zentrum für digitalen Fortschritt e.V
Chaos Computer Club e.V. (CCC)
LOAD e.V. – Verein für liberale Netzpolitik
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.
Gesellschaft für Informatik (GI) e.V.
Stiftung Datenschutz

Konsens über die Nutzung von Gesundheitsdaten

Corona-Tracing-App: rechtskonform, datensparsam und europäisch

Der Bundesverband Gesundheits-IT (bvitg) befürwortet die Entscheidung des Bundesgesundheitsministeriums für eine „Corona-Tracing-App". Gleichzeitig appelliert der Verband an alle Akteure, den Dialog über Gesundheitsdaten und ethisch vertretbare Nutzungen weiterzuführen.

Um Infektionsketten besser nachzuvollziehen und so die Ausbreitung der Covid-19-Pandemie einzudämmen, soll Deutschland eine Corona-Tracing-App bekommen. Eine entsprechende Anwendung wird derzeit federführend von der Fraunhofer Gesellschaft auf Grundlage des Softwaregerüsts DP3T (kurz für: Decentralized Privacy Preserving Proximity Tracing) entwickelt.

„Es ist ein positives Signal, dass die Bundesregierung das Potenzial digitaler Tools in der Bekämpfung der Corona-Pandemie erkannt hat und die Entwicklung aktiv vorantreibt", kommentiert Sebastian Zilch, Geschäftsführer des Bundesverbands Gesundheits-IT, die derzeitigen Entwicklungen. „Einmal mehr zeigt sich in welchem Maße digitale Anwendungen wie die Corona-Tracing-App zum Schutz der Bevölkerung beitragen können, wenn Sie datenschutzkonform und schnell umgesetzt werden. Dafür ist eine umfassende und nachhaltige Digitalisierungsstrategie allerdings ebenso notwendig wie ein sicheres, paneuropäisches Datennutzungskonzept."

Nutzenstiftenden Umgang mit Gesundheitsdaten

Aus Sicht des bvitg sind die Diskussionen um eine zentrale oder dezentrale Speicherung der Tracing-Daten als Teil eines zivilgesellschaftlichen Dialoges absolut notwendig. Andererseits hätte diese Diskussion früher und strukturierter geführt werden müssen. „Im Krisenfall über Dogmen zu streiten fördert die Verunsicherung der Menschen und kostet wertvolle Zeit. Es braucht endlich einen Konsens darüber, was eine vertrauensvolle Umgebung für den sicheren und nutzenstiftenden Umgang mit Gesundheitsdaten, deren Erhebung und auch deren Spende ist.", so Sebastian Zilch.

Zudem spricht sich der Verband langfristig für mehr Klarheit bei der Verwendung von Gesundheitsdaten aus und sieht ein klares Mandat für die neuen Mitglieder des Deutschen Ethikrats: „Derzeit zeigt sich, dass wir es uns nicht länger leisten können, das enorme Potenzial dieser Daten brach liegen zu lassen. Es wäre wünschenswert, wenn sich der Ethikrat noch intensiver mit der Nutzung von Gesundheitsdaten zum Wohle der Allgemeinheit – und nicht nur im Kontext von Epidemien – beschäftigen würde."

Sebastian Zilch, Geschäftsführer des Bundesverbands Gesundheits-IT: „Im Krisenfall über Dogmen zu streiten fördert die Verunsicherung der Menschen und kostet wertvolle Zeit."

Digitale Technologien im Kampf gegen Covid-19

Corona-Pandemie und Arbeit im Home Office

Sowohl Arbeitnehmer als auch Personalverantwortliche von Unternehmen sehen die Arbeit im Home Office grundsätzlich positiv. Das ist ein wichtiges Signal, da es dabei auch um die Akzeptanz von flexiblen Arbeitsmodellen generell geht, denn diese sind ohne Home Office kaum denkbar. Jeder fünfte Berufstätige arbeitet wegen Corona erstmals im Homeoffice.

Im Kampf gegen die Corona-Pandemie misst eine deutliche Mehrheit der Bundesbürger der Digitalisierung große Bedeutung bei. Zwei Drittel (65 Prozent) sind der Ansicht, dass digitale Technologien dabei helfen können, die Ausbreitung des Coronavirus zu verlangsamen, etwa durch Homeoffice. Das ist das Ergebnis einer repräsentativen Befragung von mehr als 1.000 Bundesbürgern ab 16 Jahren im Auftrag des Digitalverbands Bitkom. Von den berufstätigen Befragten arbeitet mittlerweile jeder Zweite (49 Prozent) ganz oder zumindest teilweise im Homeoffice. Für einige von Ihnen ist das völlig neu: 18 Prozent durften zuvor gar nicht im Homeoffice arbeiten und machen das jetzt zeitweise (15 Prozent) oder ganz (3 Prozent). Weitere 31 Prozent konnten bereits vorher im Homeoffice arbeiten und tun das jetzt häufiger (17 Prozent) oder ganz (14 Prozent). Dagegen geben 41 Prozent an, ihre Tätigkeit sei grundsätzlich nicht für Homeoffice geeignet. „Die Corona-Pandemie und die drastischen Beeinträchtigungen des öffentlichen Lebens erzwingen ein radikales Umdenken in der Kultur vieler Unternehmen. Noch stärker gefordert sind öffentliche Arbeitgeber, für die Homeoffice oft ein Fremdwort ist.

Potenziale der digitalen Technologien

Digitale Technologien sind der Schlüssel, um die Arbeitsfähigkeit von Wirtschaft und öffentlichen Einrichtungen wie Ämtern und Schulen auch in dieser außerordentlichen Krisensituation zu gewährleisten“, sagt Bitkom-Präsident Achim Berg. „Dass mobiles Arbeiten und mobiles Lernen zum Standard werden könnten, schien bislang undenkbar. Jetzt aber werden wie unter einem Brennglas die immensen Potenziale sichtbar, die digitale Technologien grundsätzlich bieten – im Kampf gegen das Virus wie auch in der Reduzierung des Berufsverkehrs und verkehrsbedingter Emissionen. Alle Unternehmen sind gefordert, Homeoffice für die dafür geeigneten Tätigkeiten einzuführen. Die Politik muss das Arbeitsrecht zwingend modernisieren, etwa indem aus der Zeit gefallene Regelungen wie die elfstündige ununterbrochene Mindestruhezeit gestrichen und der starre Acht-Stunden-Tag durch eine wöchentliche Höchstarbeitszeit ersetzt werden.“

Digitalisierung, Hygiene und Informationen

Nach Angaben der befragten Berufstätigen haben viele Arbeitgeber auf die Corona-Pandemie reagiert und setzen verstärkt auf ortsunabhängiges Arbeiten. Bei jedem dritten Berufstätigen (33 Prozent) wurde erstmals Homeoffice eingeführt, bei 43 Prozent wurden bestehende Homeoffice-Regelungen durch den Arbeitgeber ausgeweitet. Bei 45 Prozent der Berufstätigen ersetzen Telefon- und Webkonferenzen die bisherigen Treffen mit persönlicher Anwesenheit.

Weitere Maßnahmen betreffen Hygieneregeln und Informationspolitik. Klassische Umgangsformen sind tabu: 96 Prozent der Berufstätigen sagen, ihr Arbeitgeber habe Begrüßungen per Handschlag verboten. 88 Prozent wurden über persönliche Hygienemaßnahmen wie etwa regelmäßiges und häufigeres Händewaschen informiert. 29 Prozent berichten von einem speziellen Informationsangebot zur Corona-Pandemie, etwa im Intranet oder am Schwarzen Brett. Bei 22 Prozent gibt es zusätzliche Desinfektionsmittel auf Toiletten und am Eingang. Für einige Berufstätige ist die Corona-Pandemie mit erheblichen Einschnitten im gewohnten Arbeitsalltag verbunden, wie ein komplettes Empfangsverbot jeglicher Gäste am Unternehmensstandort (19 Prozent), der Absage eigener Veranstaltungen mit externen Gästen (14 Prozent), der Absage von Teilnahmen an externen Veranstaltungen wie Messen und Kongressen (11 Prozent), der Einschränkung von Dienstreisen (10 Prozent) oder einem grundsätzlichen Verbot von Dienstreisen (8 Prozent).

Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat.

Bitkom-Präsident Achim Berg: „Alle Unternehmen sind gefordert, Homeoffice für die dafür geeigneten Tätigkeiten einzuführen.“

Das Thermometer in der Hand, den Sauerstoffsättigungsmesser am Finger des Patienten und die Blutdruckmanschette direkt griffbereit. Die Werte gehen per Knopfdruck über das WLAN an die digitale Patientenkurve. Die neuen digitalen Vitaldatenmessgeräte im KRH machen es möglich.

Mehr Zeit für Pflege / Vitaldatenmessung der Zukunft

Entlastung durch Digitalisierung

In der Corona-Pandemie haben sie sich bewährt: Die neuen und im Laufe dieses Jahres an alle somatischen Kliniken des Klinikum Region Hannover ausgelieferten digitalen Vitaldatenmessgeräte sind zurzeit schon auf einigen Corona-Stationen innerhalb des KRH im Einsatz. Diese leichten Geräte sind wahre Alleskönner – auf Rollen mobil, können Blutdruck, Sauerstoffsättigung und Körpertemperatur gemessen werden. Und das Beste: Das Gerät wird in Zukunft die Daten auch direkt nach der Messung per WLAN an die digitale Patientenkurve senden.

„Es wird eine riesige Arbeitserleichterung für unsere Pflegefachkräfte", sagt Hans Röbbecke, Bereichsleiter Medizintechnik im KRH, „wo früher drei Geräte von Untersuchung zu Untersuchung geschleppt werden mussten, reicht nun das digitale Vitaldatenmessgerät. Die gemessenen Werte werden nach der Messung direkt übers WLAN in die digitale Patientenkurve übertragen. Kein lästiges Notieren und späteres Eintragen am stationären Rechner mehr, dadurch auch weniger händische Fehler."

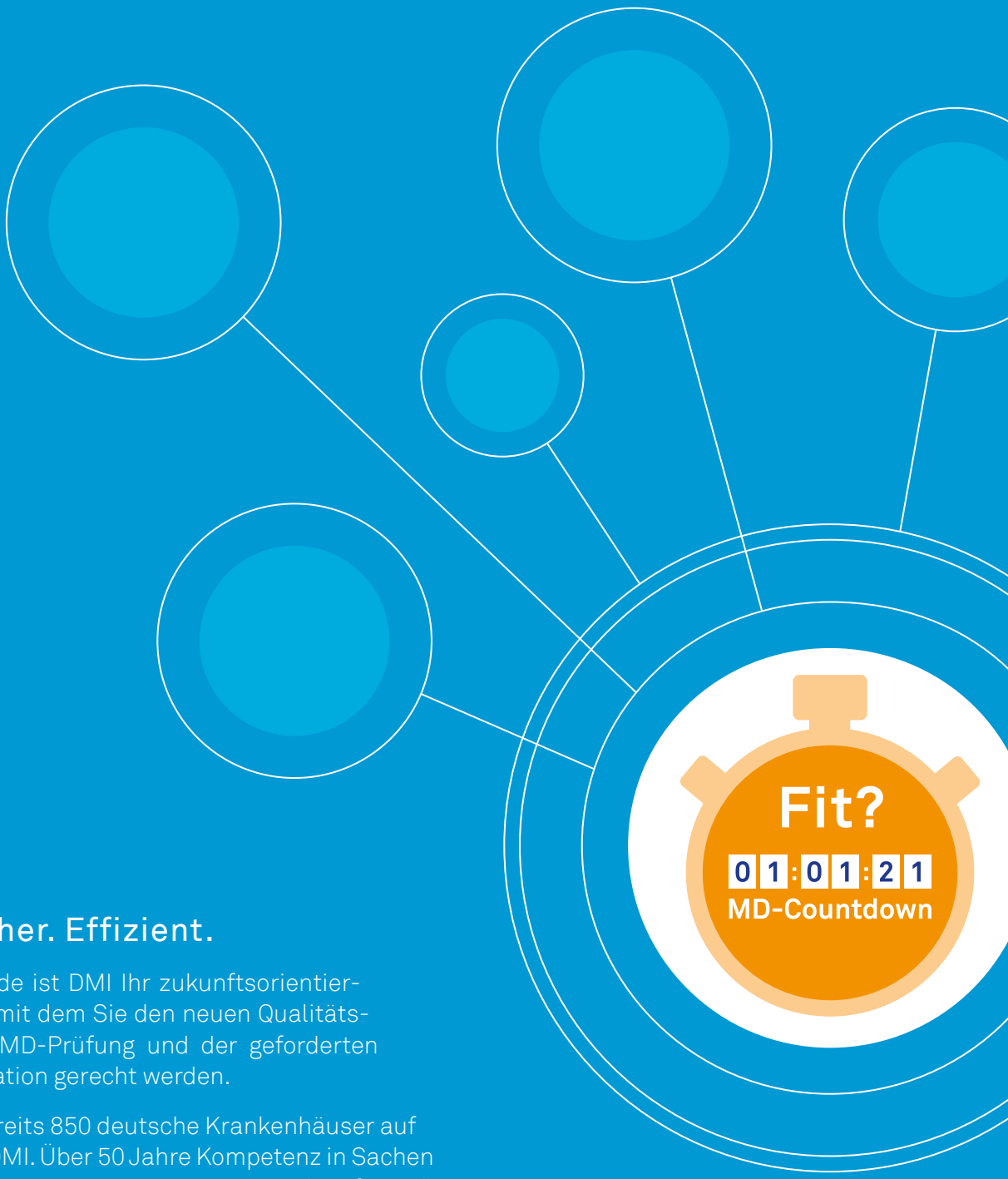
Damit werden die Untersuchungen im KRH komplett digital abgebildet und es bleibt mehr Zeit für den Kontakt mit den Patienten. Im Klinikum Siloah, Klinikum Robert Koch Gehrden und Klinikum Großburgwedel kann es bald schon mit der vollständig digitalisierten Messung und Dokumentation der Vitalparameter losgehen, die anderen Häuser folgen im Anschluss.

„Es ist ein weiterer Schritt in Richtung Pflege der Zukunft", ergänzt Michael Beurer, Leiter Zentrales Projektmanagement, „die digitalen Vitaldatenmessgeräte werden flächendeckend in allen somatischen KRH Kliniken über das WLAN mit der digitalen Patientenakte im SAP verbunden sein. Das digitale Krankenhaus ist zum Greifen nah."

Nach dem Einsatz auf den Corona-Stationen im Siloah sollen in allen somatischen KRH Häusern auf jeder Station zwei bis drei digitale Vitaldatenmessgeräte zur Verfügung stehen. „In den kommenden Monaten werden die Geräte ausgeliefert und die Pflegefachkräfte darin eingewiesen werden. Eine finale Testphase vor Beginn der Corona-Pandemie auf der Station B3 im KRH Klinikum Siloah hat keine Wünsche offengelassen. Das Feedback von den Kolleginnen und Kollegen aus der Testphase ist durchweg positiv", fügt Dr. Christian Herrmann, Abteilungsleitung Geschäftsprozessoptimierung & Anwendungsentwicklung im Bereich Informationstechnologie (IT), hinzu.

Die Einführung der digitalen Vitaldatenmessgeräte ist ein Projekt der Bereiche Medizintechnik, IT sowie des Zentralen Projektmanagements. Mit dem bald eingeführten flächendeckenden Anschluss der Geräte ans WLAN und an die digitale Patientenkurve ist ein weiterer Bestandteil der Medizinstrategie 2025 erfolgreich umgesetzt worden, in der sich das KRH Digitalisierung und dadurch Vereinfachung von Arbeitsabläufen und Entbürokratisierung auf die Fahnen geschrieben hat.

// Gut aufgestellt für Ihre digitale MD-Kommunikation.



// Einfach. Sicher. Effizient.

Mit Archivar 4.0 inside ist DMI Ihr zukunftsorientierter Lösungspartner, mit dem Sie den neuen Qualitätsansprüchen an die MD-Prüfung und der geforderten digitalen Kommunikation gerecht werden.

Vertrauen Sie wie bereits 850 deutsche Krankenhäuser auf den IT-Spezialisten DMI. Über 50 Jahre Kompetenz in Sachen informationsbasierter Prozessoptimierung sprechen für sich!

Ihr 24 h Kontakt
Tel 02534 8005-888 (Stichwort: MD21)
md21@dmi.de | www.dmi.de/md-kommunikation

D·M·I
ARCHIVIERUNG

Autonome Prozesse, neue Geschäftsmodelle, geplante Investitionen

Forderungen an SAP: Nachhaltig digitalisieren im Pandemie-Zeitalter

Die Corona-Krise hat die Defizite vieler Unternehmen bei der Digitalisierung deutlich aufgezeigt. Damit bestätigt die aktuelle Situation auch die Ergebnisse des Investitionsreports 2020 der Deutschsprachigen SAP-Anwendergruppe e. V. (DSAG), u.a. mit dem Arbeitskreis Healthcare. Demnach bewerten 63 Prozent ihr Unternehmen als „nicht sehr weit", wenn es um die Digitale Transformation geht. Digitalisierung hat viele Seiten: Auf den richtigen Dreh kommt es an: um das richtige Handwerkszeug für erfolgreiche Digitalisierungsvorhaben und die Anforderungen an SAP, um die Kunden bei ihrer Digitalisierungsreise zu unterstützen.

Die DSAG nahm in der jüngsten Umfrage geplante Investitionen für 2020 ausschließlich bei Anwenderunternehmen im deutschsprachigen Raum in den Blick. 288 CIOs, Leiter von Competence Centern (CC) und Vertreter von DSAG-Mitgliedsunternehmen in Deutschland, Österreich und der Schweiz nahmen an der Umfrage teil.

Obwohl die Unternehmen rein technologisch bereits einen hohen Digitalisierungsgrad erreicht haben könnten, zeigt sich jetzt in Krisenzeiten, wie unflexibel sie sind, z. B. wenn es um Zahlungsverfolgung, Lieferströme oder die Anpassung der Produktion an die neuen Bedingungen geht. Aus DSAG-Sicht ist ein Grund dafür, dass viele Unternehmen lediglich auf Prozessebene optimieren, die Geschäftsmodelle jedoch gleich bleiben. (1)

Dr. Marco Lenck, Vorstandsvorsitzender der DSAG: „Wenn die Unternehmen die technischen Möglichkeiten der Lösungen nicht kennen, sinkt die Bereitschaft, sich damit auseinander zu setzen."

Budgets 2021: Investitionen verschieben und neu bewerten

Marco Lenck, DSAG-Vorstandsvorsitzender, stellt fest: „Als Anwendervereinigung sehen wir in allen Branchen und Industrien unterschiedliche Konzepte, um in den Alltag zurückzukehren. Und vermutlich werden erst später im besten Fall neue digitale Geschäftsmodelle nachgefragt werden." Das läge auch daran, dass Mechanismen wie Kurzarbeit, um Gewinne und Verluste zumindest auszugleichen, noch eine Weile vorherrschen werden.

Daneben werden Unternehmen voraussichtlich Investitionen verschieben und neu bewerten, da die nötigen Mittel nicht mehr verfügbar sein werden. „Daher ist die Gefahr groß, dass insbesondere Transformationsprojekte, die erstmal wirtschaftlich nicht attraktiv sind, hinten angestellt werden. Somit ist zu befürchten, dass die Situation bei einer neuen Krise ähnlich sein wird und sich dies auch in den Budgets für 2021 widerspiegelt", lautet die DSAG-Prognose. Insgesamt rät der Interessenverband seinen Mitgliedsunternehmen vor dem Hintergrund bestehender Krisen oder noch kommender Herausforderungen in einer Welt zunehmend autonomer Prozesse, in neuen Geschäftsmodellen zu denken.

Sicherheit ist nicht optional

Ein besonders wichtiger Betriebsaspekt ist die Sicherheit. Die Wahrscheinlichkeit einer Cyber-Attacke ist heutzutage hoch und die Auswirkungen können fatal sein. Daher erwarten die Kunden von SAP die bestmögliche Unterstützung, um die Sicherheit der IT-Landschaften zu gewährleisten. Kein Fortschritt lässt sich leider noch bei der Forderung nach einem übergreifenden Security-Dashboard erkennen. „Wir erwarten, dass SAP endlich ein übergreifendes Design entwickelt und die sicherheitsrelevanten Aspekte in einem Dashboard sowohl für On-Premise-Produkte als auch für Cloud-Lösungen zusammenfasst. Sicherheit ist nicht optional", erläutert Steffen Pietsch. (2)

Planungs- und Investitionssicherheit

SAP wandelt sich von einem reinen Software-Anbieter zu einem hybriden Unternehmen mit On-Premise- und Cloud-Software im Portfolio. Um den Weg in die Cloud mitzugehen, erwarten die Kunden im Vergleich zu ihren On-Premise-Lösungen Fortschritte und keine Rückschritte. Und sie erwarten eine stabile und verfügbare Software. Das trifft auf viele SAP-Cloud-Lösungen zu. Handlungsbedarf sieht Steffen Pietsch noch bei der Verfügbarkeit der Software-as-a-Service-Lösung

für das Personalwesen SuccessFactors. „Das ist ein seit mittlerweile Jahren anhaltendes Problem. Die Stabilität muss deutlich verbessert werden. Bei einer Cloud-Lösung darf die Verfügbarkeit kein Diskussionsthema sein", gibt der DSAG-Technologievorstand an SAP weiter. Ein zusätzlicher Aspekt für die Planungs- und Investitionssicherheit sind klare, verständliche und verlässliche Roadmaps.

Leichte Trendwende bei der Digitalisierung

Neben einzelnen Produktbereichen, erfasst die Umfrage auch den Status quo der Unternehmen bei der Digitalen Transformation, unabhängig von und ohne direkten Bezug zu SAP. „Weit" und „sehr weit" sind dabei 35 Prozent der Unternehmen, eine Verbesserung gegenüber dem Vorjahr (31 Prozent), aber noch weit von den 45 Prozent aus 2018 entfernt. Für Marco Lenck eine interessante Entwicklung: „Anfangs war die digitale Euphorie groß, dann hat sich gezeigt, dass der Aufwand in manchen Bereichen doch größer ist, als angenommen. Aber die Trendwende ist zu erkennen". Dennoch hinkt die Digitale Transformation aktuell noch klar hinter den allgemeinen Erwartungen hinterher. Als „nicht sehr weit" sehen sich aktuell noch 63 Prozent und damit 3 Prozent weniger als noch im letzten Jahr.

Bessere Unterstützung– weniger Zurückhaltung

Die Gründe für die „digitale Zurückhaltung" wurden auch in diesem Jahr abgefragt. Als „wichtig" und „sehr wichtig" stehen fehlende Ressourcen wie Mitarbeiter und Berater mit 77 Prozent und die aufwendige Integration mit 68 Prozent ganz vorn. „Die Unternehmen haben erkannt, dass es komplex werden kann, wenn ein entsprechendes Projekt gestartet und die Integration vollzogen wird. Das heißt aber auch, dass SAP massiv daran arbeiten muss, die Unternehmen bei ihren Integrationsaufgaben noch besser zu unterstützen. Je standardisierter die Lösungen, desto einfacher die Integration und desto weniger Baustellen", fasst Marco Lenck zusammen.

An Technologie fehlt es nicht

An dritter Stelle steht das fehlende Know-how mit 60 Prozent. „Wenn die Unternehmen die technischen Möglichkeiten der Lösungen nicht kennen, sinkt die Bereitschaft, sich damit auseinander zu setzen. Darum ist es wichtig, die entsprechenden Abteilungen gezielt zu aktivieren", ist Marco Lenck überzeugt. Interessant ist auch der fehlende Business-Case bei 47 Prozent der Befragten. „Vielleicht sind die notwendigen Investitionen zu hoch oder der konkrete Nutzen des Projekts lässt sich nicht klar festlegen. Oder es fehlt am Know-how, was mit der Software konkret verbessert werden könnte", interpretiert Marco Lenck das Ergebnis. Denn wie die Umfrage weiter zeigt: An fehlender Funktionalität der Lösungen oder fehlender Technologie kann es nicht liegen. Die beiden Argumente stehen mit 45 Prozent bzw. 29 Prozent am Ende der Liste.

Steffen Pietsch, DSAG-Technologievorstand: „Wir erwarten, dass SAP endlich ein übergreifendes Design entwickelt und die sicherheitsrelevanten Aspekte in einem Dashboard sowohl für On-Premise-Produkte als auch für Cloud-Lösungen zusammenfasst. Sicherheit ist nicht optional."

Forderungen an SAP

Harmonisierung

- OneSAP-Experience: Benutzeroberflächen, Erweiterungskonzepte und Betriebsaspekte aus einem Guss
- Security-by-Default für alle Produkte
- Übergreifendes Security-Dashboard mit allen sicherheitsrelevanten Aspekten für On-Premise-Produkte und Cloud-Lösungen

Technische und semantische Integration

- Durchgängige, konsistent und konsequent umgesetzte API-Strategie
- Technisch und semantisch kompatible Datenmodelle
- Klare Aussagen zur Weiterentwicklung des Business Partners

Planungs- und Investitionssicherheit

- Evolutionäre Software-Entwicklung statt disruptivem Wechsel
- Klar verständliche, verlässliche und zukunftssichere Planung und Roadmap

Über die DSAG

Die Deutschsprachige SAP-Anwendergruppe e.V. (DSAG) ist einer der einflussreichsten Anwenderverbände der Welt. Mehr als 60.000 Mitglieder aus über 3.500 Unternehmen bilden ein starkes Netzwerk, das sich vom Mittelstand bis zum DAX-Konzern und über alle wirtschaftlichen Branchen in Deutschland, Österreich und der Schweiz (DACH) erstreckt.

Der AK Healthcare ist ein DSAG-Arbeitskreis (AK). Der AK beschäftigt sich neben den Themen der Patientenversorgung u.a. mit der betriebswirtschaftlichen Effizienz. Das Spannungsfeld zwischen Innovationen und den kurzfristigen Gesetzesumsetzungen erfordert die enge Zusammenarbeit mit SAP, Cerner und weiteren Softwareanbietern.

www.dsag.de,www.dsag.at, www.dsag-ev.ch

(1) DSAG-Position zur Corona-Krise: Nachhaltig digitalisieren im Pandemie-Zeitalter, 05.2020

(2) DSAG-Technologietage 2020: Digitalisierung ist alternativlos, 11.02.2020

Gestiegener Kostendruck beflügelt Geschäft bei gebrauchten Softwarelizenzen

Christian Maaßen,
Geschäftsführer SB Software-Broker GmbH

Herr Maaßen, Sie handeln mit gebrauchten Softwarelizenzen der Microsoft. Wie haben Sie bzw. Ihr Unternehmen die Auswirkungen von Covid-19 gespürt?

Zuerst sind glücklicherweise alle unsere Mitarbeiter und deren Familien gesund geblieben. Unternehmerisch hat uns, wie vermutlich jeden, Covid-19 zwar überrascht, aber wir sind ein vollständig digital aufgestelltes Unternehmen und können glücklicherweise von überall arbeiten. Es war uns somit sehr früh und ohne Abstriche möglich ins Home Office zu wechseln und von dort unsere Kunden zu bedienen.

Natürlich gab es aufgrund der Einschränkungen und vieler Unternehmen in Kurzarbeit entsprechende Rückgänge in der Nachfrage. Vor allem viele unserer Kunden aus dem Gesundheitssektor wie bspw. Kliniken haben in den ersten Wochen der Krise andere Fragen der IT-Bereitstellung beantworten müssen, als die Beschaffung der nächsten Lizenz.

Von einer Krise konnten wir als Unternehmen allerdings nicht sprechen, da im gleichen Moment die Nachfrage nach Lizenzen, die gerade für Heimarbeitsplätze erforderlich wurden wie bspw. Office und entsprechende Zugriffslizenzen, zunahmen und weiter zunimmt. Der Effekt hat sich also gegenseitig aufgehoben und verstärkt sich aktuell zu unseren Gunsten.

Anders als in den schwer vom Shutdown getroffenen Branchen wie Hotellerie und Gastronomie, haben unsere Kunden bzw. wir selbst die Möglichkeit, Umsätze zu verlagern, die in gleicher Höhe, aber eben später realisiert werden. Meint: Kunden haben IT-Projekte verschoben, aber nicht verworfen. Lizenzbeschaffungen, die für das 2. Quartal geplant und durch unsere Kunden aufgrund von Unsicherheit gestoppt wurden, leben nun wieder auf und werden in den Quartalen 3 bzw. 4 realisiert.

Erwarten Sie einen weiteren Anstieg der Nachfrage aufgrund der Mehrwertsteuersenkung bzw. wie blicken Sie auf das 2. Halbjahr?

Den gestiegenen Kostendruck spürt nahezu jedes Unternehmen und auch die Kliniken nun umso mehr. IT-Budgets waren vor der Krise bereits stark strapaziert und müssen nach wie vor zukunftsorientiert eingesetzt werden. Durch uns erreichen unsere Kunden ca. 50% Kostenreduzierung im Einkauf gebrauchter Software-Lizenzen bei gleichzeitig garantierter 100% Rechts- und Auditsicherheit durch unsere Qualitätsstandards. Aufgrund dessen blicke ich optimistisch in das 2. Halbjahr. Auch die Mehrwertsteuersenkung sehe ich als den richtigen Schritt, um den Binnenmarkt wieder anzukurbeln. Gerade bei Kliniken spiegeln 3 % weniger MwSt eine nennenswerte kfm. Größe bei der Lizenzbeschaffung wieder. Wir unterstützen dies mit unserer aktuellen Sommerkampagne und ergänzen die 3% MwSt mit weiteren 3% Skonto auf unserer ohnehin schon laufende Aktionspreise unserer Produkte. Jetzt zu kaufen, kann also weit mehr als 50% Ersparnis einbringen und ermöglicht einen zielgerichteten Mitteleinsatz der knappen IT-Budgets.

Wie erklären Sie sich, dass Unternehmen beim Thema Gebrauchtsoftware manchmal zurückhaltend reagieren?

Leider wird immer nur über die schwarzen Schafe der Branche berichtet, was nachvollziehbar ist. Der Regelfall findet selten den Weg in die Presse. Dennoch haben wir einen großen und stabilen Markt, der durch seriöse Partner bedient wird und durch das EuGh entsprechend legitimiert und genau spezifiziert wurde.

Meist gilt es allerdings die individuellen Fragen auf Kundenseite bspw. von Juristen, Einkauf und Lizenzmanagement vollständig zu beantworten und sich mit dem Thema vertraut zu machen, sowie uns als Businesspartner kennenzulernen. Zweifel kann man, meiner Meinung nach, nur über Vertrauen und Transparenz aus dem Weg räumen. Vertrauen in uns und gerade in unsere Vorgehensweise bekommt der Kunde durch diesen Prozess. Transparenz schaffen wir über unseren Marktantritt: Bei uns erhält der Kunde den gleichen Grad an Transparenz von uns wie ihn der Ersterwerber selbst erlangt hat. Keine Blackbox, kein Testat. Schlicht alle Dokumente im Original.

Schlagenden Argumente sind somit das Vertrauen in uns als Partner und der Grad an Transparenz unserer Dokumentation, egal ob mit Covid-19 oder ohne.

Kontakt:
SB Software-Broker GmbH
Hüserheide 52
47918 Tönisvorst
Tel.: +49 2 11 54 76 71 20
Fax: +49 2 11 54 76 71 21
info@software-broker.com
www.software-broker.com

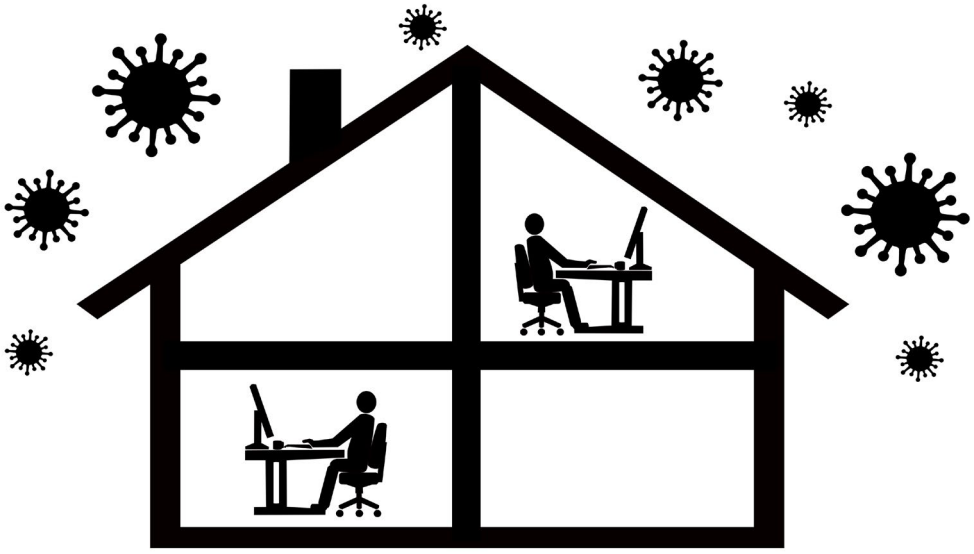
Corona Warn-App – jetzt ist sie da!!

Was lange währt...ist seit dem 16. Juni nun erhältlich: die deutsche Corona-App. Geplant war sie eigentlich schon für den April, aber manche Entscheidungen müssen eben genau abgewogen werden und viele Kanäle durchlaufen.

Nun können und sollen sich die Nutzer die deutsche Corona-Warn-App im Google Play Store oder im Apple Store herunterladen. Unterstützt werden die Betriebssysteme ab iOS 13.5 (also ab iPhone 6s und iPhone SE) sowie ab Android 6 (d.h. ab Marshmallow) und Google Play Services.

Mit der App können Menschen anonym und schnell darüber informiert werden, wenn sie sich in der Nähe eines Infizierten aufgehalten haben. „Je mehr Menschen die Corona-Warn-App nutzen, desto schneller können in Zukunft Infektionsketten durchbrochen werden.“, betont die Bundesregierung. "Die App ist kein Allheilmittel, aber ein wichtiges Instrument, um das Virus einzudämmen. Das geht am besten, wenn viele mitmachen. Das Virus können wir nur im Teamspiel bekämpfen", so Bundesgesundheitsminister Jens Spahn. Die Nutzung ist komplett freiwillig, doch der Gesundheitsminister appelliert an die Eigenverantwortung der Bürger. SAP und Telekom-Systems haben gezeigt, dass sie in kurzer Zeit diese App entwickeln konnten. Sie garantieren absolute Sicherheit und hohen Datenschutz. Die Deutsche Krankenhausgesellschaft (DKG) sieht die Corona-Warn-App als weiteren Baustein der Bekämpfungsstrategie gegen die Ausbreitung des Corona-Virus und empfiehlt Mitarbeiterinnen und Mitarbeitern in Krankenhäusern ausdrücklich deren Nutzung.

Nun muss sich die App in der Praxis bewähren und dazu müssen vor allem möglichst viele Leute diese App nutzen. Dies kann helfen, die Infektion einzudämmen und somit möglichst bald wieder zu einer Art normalem Leben zurückzufinden. *df*



Homeoffice für die IT-Abteilungen – Lehren aus der Krise

Nach Beginn der Corona-Krise war das Stichwort „Homeoffice“ ganz schnell in aller Munde. Glaubt man einschlägigen Medienberichten, dann wechselten im April etwa ein Drittel der Beschäftigten in Deutschland ins Homeoffice. Diese Virtualisierung der Arbeitswelt bringt natürlich auch immense Herausforderungen für die IT mit sich. Gerade in chronisch unterfinanzierten Bereichen wie der Krankenhaus-IT ist eine solche Umstellung innerhalb weniger Tage bis Wochen nur sehr schwierig zu realisieren, ganz zu schweigen von der Umsetzung der nach wie vor gültigen Daten- und Arbeitsschutzvoraussetzungen.

In diesem Artikel soll es aber weniger um diese Thematik gehen, sondern vielmehr um die Frage, welchen Stellenwert das Homeoffice für die IT-Abteilungen selbst hat. Wie geht die Krankenhaus-IT für sich selbst mit diesem Thema um?

Zunächst einmal lässt sich sicherlich feststellen, dass wohl die meisten Kollegen aus der Krankenhaus-IT in der einen oder anderen Form schon seit vielen Jahren gewohnt sind, auch von zu Hause aus zu arbeiten. Der Beruf bringt es so mit sich, dass Tätigkeiten teilweise zu unchristlichen Zeiten, am Abend, in der Nacht, am Wochenende erbracht werden müssen. Da ist es nicht immer wirtschaftlich und sinnvoll, dass der betroffene Mitarbeiter dafür ins Büro fährt, umso mehr, wenn er zuvor schon seinen regulären täglichen Dienst vor Ort geleistet hatte. Im Rufbereitschaftsdienst ist es sogar regelhaft in praktisch allen Krankenhäusern so, dass IT-Dienstleistungen wenn möglich remote erbracht werden. Schon zu Zeiten, als das Wort Homeoffice sich noch gar nicht in der Breite durchgesetzt hatte, wurde das pragmatischerweise so gelebt.

Gewohntes über Bord werfen

Die Zeiten haben sich seither und auch schon lange vor Corona geändert, und es gab immer mehr Mitarbeiter auch aus anderen Bereichen, vor allem der Verwaltung, später auch in der Medizin, die teilweise Tätigkeiten von außerhalb des Unternehmens geleistet haben. Das führte dann in den Köpfen der Entscheidungsträger zu der Einsicht, dass auch der Arbeitsplatz fern des Unternehmens geregelt werden muss. Die bis dahin vorhandenen Regelungen für IT-Mitarbeiter waren eher informaler Natur. Man ging implizit davon aus, dass der IT-Mitarbeiter umfassende Rechte braucht und zu Hause sowieso über das notwendige Equipment und Internetanschluss verfügt. Erst in den letzten Jahren sind dann formalisierte interne Dienstvereinbarungen und Checklisten entstanden, um Heimarbeitsplätze definieren und genehmigen zu können. In manchen Krankenhäusern ist das bis heute noch nicht konsequent umgesetzt.

In der Corona-Krise wurde, wir haben das alle am eigenen Leib erlebt, schnell ganz vieles anders und Gewohntes

über Bord geworfen. War man bisher gewohnt, dass die Geschäftsführung gern die IT-Fachkräfte nach Möglichkeit vor Ort versammelt haben wollte, damit die Feuerwehr in Sachen IT jederzeit schlagkräftig einsatzbereit sein konnte, kehrten sich nun plötzlich manche Rahmenbedingungen regelrecht um. Was wäre, wenn plötzlich der Corona-Virus unter den IT-Mitarbeitern grassieren würde und diese reihenweise ausfielen, entweder tatsächlich krank und in vorbeugender Quarantäne? Ein Fall in der IT-Abteilung genügt möglicherweise, und man kann die gesamte IT-Belegschaft nach Hause schicken.

Das nun aber funktioniert natürlich nicht, denn gewisse Dienstleistungen müssen vor Ort erbracht werden. Einen Drucker aufzustellen und zu konfigurieren oder ein Netzwerk zu patchen macht sich nun einmal aus dem Homeoffice ziemlich schlecht.

So hat auch hier die Analyse begonnen: Wen brauche ich denn zu was vor Ort, und wer arbeitet besser zu Hause?

Aufgaben zunehmend aus der Ferne lösen

Wie in der Corona-Krise allgemein üblich, hat sich zunächst jeder schnell seinen individuellen Weg gesucht. Als eine Art Best Practice hat sich jedoch abgezeichnet, die Mitarbeiter so geschickt zwischen Präsenzdiensten im Krankenhaus und Homeofficekollegen zu verteilen, dass einerseits immer genug Manpower für notwendige Aufgaben vor Ort vorhanden ist, andererseits aber der andere Teil von zu Hause arbeiten kann, um Infektionsrisiken zu entgehen. Im Idealfall kann man dieses System sogar rotierend einführen, so dass der Großteil der Mitarbeiter abwechselnd wochenweise zu Hause und dann wieder vor Ort eingesetzt wird.

Generell ist es in der IT schon seit Jahren so, dass sich Aufgaben immer mehr aus der Ferne lösen lassen. Das ist auch unabdingbar, weil es in früheren Zeiten im Verhältnis zu den vorhandenen Personalressourcen viel zu lange gedauert hatte, Mitarbeiter vor Ort zum Anwender zu schicken, umso mehr nach der Konsolidierungswelle mit der Gründung von Gesundheitsverbünden mit teilweise erheblichen Fahrstrecken und -zeiten zwischen den einzelnen Standorten. Der Trend geht tatsächlich zunehmend in die Richtung, dass nur noch mit Hardware vor Ort zusammenhängende Dienstleistungen, das sind in der Regel die Clients und das Netzwerk, nicht remote erbracht werden. Die Fülle der Aufgaben ließe sich anders gar nicht mehr bewältigen. Es scheint auch über die Jahre ein gewisser Gewöhnungseffekt bei den Anwendern daran eingetreten zu sein. Hörte man in der Vergangenheit am Hotlinetelefon erst einmal den verzweifelten Ruf „Da muss sofort jemand vorbei kommen. Hier geht gar nichts mehr“, sehen das auch die Betroffenen Kräfte in der Medizin inzwischen anders. Der zugehörige Spruch bei der Hotline heißt mittlerweile eher „Ich hab da ein Problem, können Sie sich man kurz aufschalten?“

Zumindest bis vor der Coronakrise konnte man aber beobachten, dass trotzdem die Mitarbeiter fast ausschließlich im Krankenhaus arbeiteten und nicht im Homeoffice, obwohl intern kolportiert wurde, das meiste könne man eigentlich auch von irgendwo her machen. Wäre es also nicht die logische Konsequenz, wenn zukünftig regelmäßig die halbe Belegschaft in der IT im Homeoffice arbeiten würde? Ein Frage, die sich als Lehre aus der Krise ja übrigens allgemein im Arbeitsmarkt stellt. Es könnten so immerhin viele Reisezeiten gespart und der vielbeschworene Verkehrskollaps auf unseren Straßen verhindert werden. Ob es allerdings dazu kommen wird, das kann wohl im Moment noch niemand voraussagen. Nicht zu unterschätzen sind nämlich auch andere Faktoren wie der doch einfachere schnelle Austausch mit den Kollegen im Großraumbüro, der soziale Aspekt der Arbeit für den Menschen und die Schwierigkeiten im Homeoffice, wenn sich rund um den Schreibtisch und das Arbeitszimmer die gesamte restliche Familie bewegt.

Es sind auf jeden Fall neue Konzepte gefragt, und Corona sollte im eigentlichen Wortsinn „Krise“ auch als Chance verstanden werden, Dinge in Zukunft anders und besser zu machen.

Horst-Dieter Beha, Vorsitzender KH-IT-Leiterverband

Medical Device Regulation (MDR) geht die Krankenhaus-IT sehr viel an

Die bereits Mitte 2017 in Kraft getretene MDR entfaltet ab 26.Mai 2020 ihre volle Wirkung. Da sich die Auswirkungen nicht nur auf Hersteller von Medizinprodukten, sondern auch auf Anwender von Krankenhaus-IT erstreckt, beschäftigte sich ein Vortrag von Dipl.-Ing. Ulrich Wieland vom DRK-Krankenhaus Lichtenstein auf der Herbsttagung 2019 in Erlangen mit dieser Thematik.

Wieland, der als Beirat für Konvergenz BMT-IT Mitglied des Vorstandes im Bundesverband KH-IT ist, verwies darauf, dass die MDR nicht nur die Anforderungen an Zulassung und Marktbeobachtung von klassischen Medizinprodukten stark erhöht, sondern diese auch auf Software ausweitet, die zur Diagnose und Therapie von Krankheiten entwickelt wurde.

Konkret müssen Hersteller, die solche Software entwickeln, neben der Registrierung der Software bei der EURAMED-Datenbank und der Kennzeichnung mit einer eindeutigen Unique Device Identifikation (UDI) u.a. strenge klinische Überwachungen nach dem Inverkehrbringen sowie Prüfungen nach jedem Software-Update sicherstellen.

Dadurch wird im Grunde zukünftig für jeden Softwarehersteller – also u.U. auch IT-Abteilungen von Kliniken selbst – ein Risikomanagementsystem nach ISO 13485:2016, erforderlich, sobald die entwickelte Software dazu bestimmt ist „Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden kann."

Umgangen werden könne dies nur, wenn der Hersteller ausdrücklich im Bestimmungszweck ausschließt, dass die Software

zur Diagnose, Therapie oder Überwachung von Krankheiten, Behinderungen oder Verletzungen oder

- zur Empfängnisregelung oder
- zur Untersuchung bzw. Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs

vorgesehen ist. Nur wenn in der Medizin eingesetzte Software also lediglich

- zur Dokumentation
- für rein administrative Zwecke
- zu Wellnesszwecken,
- als Zugang zu Fachliteratur oder
- für medizinische Berechnungen

dienen soll, wäre eine Qualifizierung als Medizinprodukt nicht erforderlich. Allerdings verweist Wieland darauf, dass dies dann nicht nur in der Zweckbestimmung, sondern auch auf werbenden Websites, der Bedienanleitung sowie auf Flyern und Messen ausdrücklich Erwähnung finden müsste.

Autor: Ulrich Wieland, DRK-Klinikservicegesellschaft Sachsen mbH, wieland@kh-it.de

Die Corona-Pandemie aus dem Blickwinkel der Krankenhaus-IT – was war, was ist und was sollte werden?

Mit den Bildern aus Bergamo, der unmittelbar vor der Haustür greifbaren Bedrohung der Bevölkerung durch ein derzeit nicht mit Medikamenten besiegbares Virus, gewann nach den ersten Covid-19-Fällen in der Bundesrepublik ein Aktionismus Dynamik, der bis dahin nicht bekannt war.

Ein Land wurde heruntergefahren und nahezu zum Stillstand gebracht. Nicht vorstellbare Möglichkeiten des alltäglichen Lebens wie Betreuung der Kinder daheim inklusive der Eltern als Neulehrer, Kontaktbeschränkungen, arbeiten von zu Hause wurden über Nacht Realität.

Aber vor allem die Gesundheitsversorgung und hier vor allem die Krankenhäuser rückten in den Fokus. Binnen weniger Tage wurden Bettenkapazitäten geschaffen, Medizingeräte für die Beatmung geordert, sofern überhaupt möglich. Krasse Versäumnisse der Politik aus der Vergangenheit wurden transparent und mit viel Symbolik, warmen Worten und Aktionismus kaschiert.

Es fehlte an Schutzmitteln, so billigen Dingen wie Mundschutz und Desinfektionsmittel. Horrende Preise wurden bezahlt, um wenigstens einigermaßen den Anforderungen gerecht zu werden. Für alle sichtbar wurde dies mit der zunächst heruntergespielten Bedeutung der Masken für den Schutz vor dem Virus, die dann größer wurde, als die Masken vorhanden waren oder die Leute anhand der zahlreich veröffentlichten Nähanleitungen selbst welche herstellten.

Die Personaleinsatzplanung im medizinischen Bereich der Kliniken wurde angepaßt, 12-Stunden-Schichten in abwechselnden Kohorten sollte eine bestmögliche Patientenversorgung sicherstellen. Schnell machte der Begriff „unsere Helden" die Runde, die Politik versprach in Anbetracht der unbekannten und nicht kalkulierbaren Situation Anerkennung, von der mittlerweile zumindest für die stationären Pflegekräfte nichts mehr übrig ist. Bleibt die Hoffnung, daß die Pflege sich nach der Coronazeit ihrer Bedeutung und ihrer Macht bewußt wird, um Versprochenes vehement einzufordern und sich nicht mit warmen, leeren Worten abspeisen zu lassen.

Wertschätzung politisch Verantwortlicher ist offensichtlich nur so lange gegeben, bis man nicht mehr auf die Wertzuschätzenden existentiell angewiesen ist.

Und wo blieb bei all dem die immer wieder geforderte Digitalisierung des Gesundheitswesens? Welche Nachteile oder auch Vorteile zeigten sich aufgrund vorhandener oder fehlender digitalisierter Abläufe in den Kliniken?

Zunächst wurden die meist rudimentär vorhandenen Möglichkeiten des Zugriffs von zu Hause soweit ausgebaut, daß mobiles Arbeiten ermöglicht wurde. Mangels fehlender Betriebsvereinbarungen und Regelungen für einen „HomeOffice"-Arbeitsplatz mit all seinen gesetzlich bedingten Vorgaben, war das mobile Arbeiten der kleinste gemeinsame Nenner.

Ebenso schnell waren dann Video- und Telefonkonferenzlösungen eingerichtet. Meist mit datenschutzbedenklichen Lösungen wie Zoom, Teams, WebEx aus der Cloud, aber in Anbetracht der Bedrohungslage wurde kurzerhand Datenschutzvorgaben ignoriert und dem reinen Pragmatismus untergeordnet.

Mit den Konferenzlösungen konnten zumindest die mobilen Verwaltungsarbeiter ihrer gewohnten Tätigkeit nachgehen. Die Lösungen wurden auch in den Physiotherapie-Bereichen genutzt, ebenso für Videosprechstunden oder auch für telemedizinische Anwendungen.

IT-Abteilungen in Krankenhäusern mit einer Krankenpflegeschule sahen sich wie die allgemeinen Bildungseinrichtungen mit der Herausforderung konfrontiert, Fernunterricht jenseits der Präsenzveranstaltungen zu ermöglichen. Auch hier mußten teilweise die schnellen Übernachtlösungen der Schulen wieder eingefangen und auf datenschutz- und sicherheitstechnisch annehmbare Basis gestellt werden.

Weiterhin mußten Anpassungen in den Informationssystemen der Kliniken vorgenommen werden, um die Vorgaben z.B. der internen Hygiene und der Gesundheitsämter zu erfüllen. Das betraf die Triagierung der aufgenommenen Patienten und somit ihrer Risikoerhebung bzgl. Covid-19-Infektion und es betraf die Meldungen über freie und belegte Betten in den Ausprägungen Normalstation und Intensivbetten, wobei dann noch zwischen beatmeten und nicht beatmeten Patienten unterschieden wurde.

Offensichtlich sind die durchaus digital erhobenen und weitergeleiteten Daten nicht medienbruchfrei ans RKI weitergeleitet worden. Wie sonst erklärt sich, daß dieses immer wieder seine Zahlen korrigieren mußte mit dem Verweis auf noch nicht aus allen Ländern vorliegenden Zahlen? Hier ist offensichtlich die Notwendigkeit zur digitalen Verbesserung der Abläufe gegeben. Gesicherte Daten sind in der Pandemie-Situation das wichtigste Gut für klare und transparente Entscheidungen. Wenn das nicht gelingt, werden Entscheidungen spekulativ wie mit einem Blick in die Glaskugel getroffen oder es gewinnt der Experte mit den vermeintlich besten Argumenten, aber nicht immer den richtigen. Das föderale System ist hierbei entgegen aller Verlautbarungen dann doch eher hinderlich als sinnhaft.

Ansonsten wurden nahezu alle laufenden Projekte auf Eis gelegt. So auch die eigentlich nötigen Maßnahmen zur Anbindung der Krankenhäuser an die Telematikinfrastruktur. Hatte die jemand in den Corona-Hochzeiten vermißt?

Was bleibt nach der Corona-Zeit übrig? Welche Erkenntnisse sollten zu innovativen und nachhaltigen Verbesserungen führen?

Die Politik hat in der Pandemie-Prävention versagt. Erkenntnisse aus der 2012 erfolgten Analyse von Katastrophenszenarien wurden nicht in Handlungen und Maßnahmen umgesetzt. Lediglich dem Umstand, daß Nachbarländer und Italien die ersten stark betroffenen Regionen mit den schwerwiegenden Folgen in der Gesundheitsversorgung und die Bundesrepublik grundlegende Erfahrungen von dort kurzfristig umgesetzt hat, ist es zu verdanken, daß wir vor der eigenen Haustür keine Kolonnen von Leichenwagen und überlastetes Klinikpersonal gesehen haben. Es war reines Glück. Es bleibt zu hoffen, daß die prognostizierte zweite Welle ebenso glücklich überstanden wird. Allerdings sollte dann auch noch rasch und ohne unnötige Diskussion die Anerkennung und Wertschät-

zung insbesondere der Pflege erfolgen, damit sie auch weiterhin hochmotiviert arbeiten.

Gezeigt hat sich, daß Digitalisierung zum abstrakten Buzzword geworden ist, inflationär genutzt, ohne vorstellbare Inhalte. Den Fachleuten in den IT-Abteilungen war schon immer bewußt, daß hier nur von einem Mittel zum Zweck gesprochen wurde. Aber die Frage nach dem Sinn und dem Ziel kaum diskutiert, geschweige denn mit Inhalten beantwortet wurde.

Deutlich wurde, die vorhandenen IT-Lösungen sind ausreichend das Mindestmaß an Prozeßunterstützung zu gewährleisten. Die KIS-Lösungen sind in der Lage relevante Daten zu liefern.

Die Corona-Zeit sollte anregen, inne zu halten. Was braucht es sinnvoll an digitalen Prozessen. Wem soll damit geholfen werden? Wem soll es nützen?

Die Telematikinfrastrukur ist in ihrer zugrunde liegenden Idee einer Vernetzung des Gesundheitsbereichs über die leider bestehenden Sektorengrenzen hinaus eine gute und sinnvolle Idee. Das Bild der Datenautobahn paßt hierbei durchaus.

Zu hinterfragen ist, welche Fahrzeuge diese Autobahn nun zuerst und dann zunehmend nutzen sollen.
Der Abgleich und die Aktualisierung versicherungstechnischer Daten mit den Kassen ist aus administrativer Sicht ein richtiger Schritt, auch weil er die TI-Basis geschaffen und relativ einfach umzusetzen war.

Mit den Pandemie-Erfahrungen sollten Dienste in den Fokus gerückt werden, die derzeit nur rudimentär in der Umsetzung stehen. Dazu zählen u.a. das eRezept, der elektronische Medikationsplan, die elektronische AU – in den Lockdown-Wochen ein wirksames Mittel durch telefonische AU den Ansturm auf die Hausärzte zu minimieren – und der elektronische Arztbriefversand zwischen Kliniken und niedergelassenen Ärzten.

In der Folge der eRezept- und Medikationsplanbereitstellung könnte auch die für den Patienten am besten nachvollziehbare und sinnhafte Prüfung von verordneten und genommenen Medikamenten erfolgen und er sowie sein Hausarzt auf Wechselwirkungen und Nachteile der Medikation hingewiesen werden. Die Arzneimitteltherapiesicherheit (AMTS) wäre nicht nur Hülle, sondern im Sinne einer besseren Gesundheitsversorgung Wirklichkeit.

Ob der elektronischen Patientenakte in dem Zusammenhang die große Bedeutung zukommt, darf bezweifelt werden. Vor allem aufgrund der noch fehlenden Strukturen, definierten Inhalte und Berechtigungs- und Rechtevergabekonzepten würde die Akte im ersten Schritt mit den heute verfügbaren Möglichkeiten eher der weniger sinnvollen PDF-isierung folgen und keinen Mehrwert bieten.

Schließlich bleibt bei allem die Frage ungeklärt, wer soll das bezahlen? Die Länder und die Kassen kommen seit Jahren nicht ihren finanziellen Verpflichtungen nach, gemäß ihren Rollen die Krankenhäuser mit den nötigen Mitteln auszustatten. Spannend zu sehen wird sein, ob und wie die kurz vor der Corona-Zeit wie in der Bertelsmannstiftung empfohlenen Klinikschließungen weiter diskutiert werden oder ob sich die Politik traut, vom kommerziell aufgestellten Gesundheitsunternehmen hin zu einem der Allgemeinheit geschuldeten Gesundheitswesen umzusteuern. Dabei müssen auch andere Vergütungs- und Abrechnungslösungen gefunden werden. Der Schweregrad eines Falls oder die Liegedauer eines Patienten sind hierfür sicherlich nicht das Maß der Dinge.

Auch müssen die zunehmenden neuen Kostenbereiche wie die IT angemessen in die Kalkulationen und bereitgestellten Budgets der Länder und Kassen einbezogen werden. Es sind nicht nur Investitionen, um die es geht. Der Großteil der Gelder wird für den Betrieb und hier auch für die Erfüllung von Sicherheit und Datenschutz ausgegeben. Interessant wäre in dem Zusammenhang die Frage, wieviel Euros in dem Zusammenhang aufgewendet werden müssen, um einen Euro unmittelbar in einen digitalisierten Prozeß auszugeben.

Nicht unberücksichtigt bleiben darf auch die Industrie, die letztlich mit ihren Software- und Hardwarelösungen erst die elektronischen Verfahren ermöglicht. Hier sollte es aber nicht, wie der Eindruck in der TI-Umsetzung entsteht, darum gehen, Konjunkturprogramme für die Unternehmen aufzulegen und Profitoptimierungen zu ermöglichen.

Fazit

Die Corona-Pandemie sollte als Zäsur verstanden werden, bisher als selbstverständlich vorangetriebene Digitalisierung von Prozessen in den Krankenhäusern auf ihren Sinn und Zweck zu hinterfragen. Es ist der Mut aufzubringen, Vorhaben zu priorisieren, die nachweislich und unmittelbar für die eigentliche Zielgruppe von allem – den Patienten – Nutzen generiert.

Die Finanzierung aller damit verbundenen Kosten darf nicht in zäher und basartypischer Weise verhandelt werden, die Gelder sind bereitzustellen oder die Ziele sind zu streichen.

Und es bleibt zu hoffen, daß die Politik die Angst nicht vergißt, als Corona plötzlich vor der Tür stand, und im Sinne einer bestmöglichen Pandemievorbereitung das Gesundheitswesens mutig umbaut. Die Frage ist nicht, ob sondern wann das nächste Virus auftritt, für das es noch keine Medikamente gibt.

Autor: Reimar Engelhardt, Vorstand KH-IT e.V.

Digitalisierung im Krankenhaus: Ist das digitale Krankenhaus wirklich die sinnvolle Vision für die Zukunft ? Oder ist das nur wieder eine Marketingfahne der IT-Firmen ?

Die Corona-Pandemie hat es gezeigt: wenn es sein muss, geht Digitalisierung extrem schnell. Plötzlich können viele Arbeitnehmer aus dem Homeoffice arbeiten. Plötzlich gibt es die AU per Telefon oder die Sprechstunde beim Arzt per Video und Internet.

Mehr als eine Fachzeitschrift spekulierte schon, dass das Corona-Virus den größten Digitalisierungsschub ausgelöst hätte.

Welche Veränderungen brachte Corona für die Krankenhäuser ?

Zunächst einmal wurden die Krankenhäuser dazu verpflichtet, ihre Betten von allen nicht dringenden Fällen frei zu räumen, um Platz für Corona-Patienten zu schaffen. Ein elektronisches Meldeverfahren für freie Intensivbetten wurde eingeführt – Teilnahme am elektronischen Verfahren nicht verpflichtend. Ärztliches und pflegerisches Personal wurde zum Präsenzdienst verdonnert, die Reinigungskräfte ebenso. Alle anderen Berufsgruppen wurden nach den jeweiligen Funktionen und Bedarfen nach Hause geschickt oder arbeiteten nach wie vor im Krankenhaus.

Bei welchen Prozessen ist die fehlende Digitalisierung im Krankenhaus aufgefallen ?

Eigentlich ist die fehlende Digitalisierung im Krankenhaus in der Corona-Pandemie kaum aufgefallen. Die Ursache dafür liegt – positiv formuliert – in der Resilienz der Krankenhaus-Prozesse gegen technische Störungen. Patientendaten liegen nicht elektronisch vor ? Kein Problem, ein Zettel ist schnell gefunden und die Daten noch schneller notiert.

Natürlich gibt es wichtige Kernprozesse, wie die verschiedenen diagnostischen Verfahren (u.a. Labor, Radiologie, Pathologie…), bei denen es ohne Computer nicht geht. Auch dafür werden hoch resiliente Systeme genutzt, auch dort gibt es bewährte und geübte Ersatzverfahren, wenn die Technik streikt.

Wozu dann eigentlich weitere Digitalisierung im Krankenhaus?

Das ärztliche und pflegerische Personal setzt IT nur im unbedingt notwendigen Umfang ein, außer es gibt IT-Systeme die Abläufe unterstützen, die dem jeweiligen Protagonisten gerade besonders wichtig sind. Da dies aber schon in einem Haus sehr viele unterschiedliche Anwendungsfälle sind, kann keine kritische Masse der Anforderungen entstehen.

Die Klinikleitung betrachte die IT oft noch als „kostenträchtige EDV", die immer nur Geld will und keines bringt. Den strategischen Nutzen, die Effizienz- und Qualitätspotentiale die ein sinnvoller IT-Einsatz bringen kann, wurden bis heute nicht verstanden. Ergänzungen oder Veränderungen des Leistungsspektrums werden daher ohne jede Berücksichtigung der IT geplant, die dann natürlich als gefühltes ko-Argument mit Kosten für Schnittstellen und Systeme und Wartung und Personal… um die Ecke kommt.

Gemeinsam mit Prozess-Managern, die keine Ahnung von IT aber viel Ahnung von (uralten, aber funktionierenden) Abläufen haben, wird eifrig weiter an einem antiken Krankenhaus gebastelt, das bereits heute zum Tode verurteilt ist. Sie haben es nur noch nicht gemerkt.

Aber auch auf Seiten der zentralen Organisationen, wie Kostenträger, Gesundheitsministerien, Krankenhausverbände, Trägerorganisationen, hängt man der Vision des Krankenhaus 4.0 nach. Die Marketingfanfaren der verschiedenen Anbieter feiern mit schmissiger Musik Visionen, deren Umsetzung kostengünstig zu haben sein soll und deren Betrieb fast schon kostenlos ist.

Spätestens hier krachen Welten aufeinander, merkwürdigerweise ohne, dass die Akteure das merken. Wie soll Digitalisierung, die immer etwas mit der Umsetzung manueller Prozesse auf IT-Systeme zu tun hat – und damit ganz stark von Standardisierung lebt, in einer Umgebung funktionieren in der schon der simple Prozess der administrativen Aufnahme von Patienten in jedem Haus anders gehandhabt wird ? In dem das Leben der Patienten davon abhängt, dass der Anamnesebogen des Chefarztes genau so aufgebaut ist, wie sein seit Jahrzehnten liebevoll gepflegter Freßzettel – nur jetzt eben als elektronischer Freßzettel ?

Ein unsinniger manueller Prozess ist digitalisiert immer noch ein unsinniger Prozess – wenn er bei dieser Verwandlung nicht auch grundsätzlich an die Möglichkeiten der Technik angepasst und überarbeitet wird. Genau das passiert aber höchst selten. Die Veränderungsbereitschaft und der Willen zur Veränderung sind leider sehr unterschiedlich in der Gesundheitsbranche verteilt.

Weiteres Effizienzpotential wird verschwendet, da die Möglichkeiten der IT meist nicht in Betracht gezogen wurden. Überspitzt formuliert: die Patientendaten werden auch bei einem vernetzten Ultraschallgerät noch von Hand am Gerät eingegeben, weil der Prozess der elektronischen Leistungsanforderung mit Übermittlung der Patientendaten ans Medi-

zingerät bei den anfordernden Menschen keine ausreichend Akzeptanz gefunden hat.

Historisch gewachsene und von persönlichen Erfahrungen geprägte Abläufe, gepaart mit der Ignoranz der Entscheidungsträger und der technischen Inkompetenz der Funktionsträger führen zu einer zementierten und höchst ineffizienten IT-Landschaft im Krankenhaus.

Im Ergebnis darf die IT dann die aufgrund guten Marketings verkauften IT-Neuheiten in Empfang nehmen und gefälligst sofort einbauen. Störungsfreier Betrieb, auch einer uralten Infrastruktur wird selbstverständlich erwartet. Datenschutz und IT-Sicherheit werden als Ausreden der IT wahrgenommen, die „intelligenten" und „technisch eleganten" Lösungen der Fachseite nicht umsetzen zu müssen. Was natürlich aus Sicht der IT Unsinn ist…

Was wäre der bessere Ansatz ?

IT im Krankenhaus ist genauso wenig wie die Digitalisierung Selbstzweck. Der Einsatz von IT sollte immer dazu dienen Prozesse im Hinblick auf Effizienz, Effektivität und Qualität zu verbessern. Wo die Technik es erlaubt, ist dazu die Digitalisierung von Prozess-Schritten sinnvoll.

Das bedeutet, bestehende Prozesse daraufhin zu prüfen, ob und wie sie durch Einsatz von IT verbessert werden können. Die Menschen, die entlang dieser Prozesse arbeiten, müssen sich auf die Technik einlassen, versuchen sie zu verstehen. Umgekehrt muss die IT versuchen, die Abläufe zu verstehen, um sinnvolle Vorschläge für die Prozessoptimierung machen zu können. Das Ergebnis sollte dann ein guter (effektiver) Prozess sein, der durch den Einsatz der IT effizienter ist als der bisherige manuelle Prozess. Die Vermeidung von Systembrüchen sichert dann die Datenqualität.

Der springende Punkt ist die nächste Abstraktionsebene: solchermaßen optimierte Prozesse und die darunter liegenden Systeme können vernetzt werden und damit plötzlich noch deutlich mehr Nutzen stiften. Im Kern: wo immer möglich sollte Automatisierung dem Menschen unnütze Arbeit abnehmen und so Freiraum schaffen, sich mehr mit den Patienten zu befassen.

Das ist Digitalisierung im Krankenhaus. Die meisten bisherigen Ansätze sind nur alter Wein in neuen Schläuchen.

Autor: Jürgen Flemming, Pressereferent, Mitglied im Vorstand des KH-IT e.V.

Herbsttagung als Präsenzveranstaltung geplant

Im Rahmen einer "Blitzumfrage" zur Durchführung der Herbsttagung als Präsenzveranstaltung, hat sich mit knapp 69% eine deutliche Mehrheit der 190 Umfrageteilnehmer für eine Präsenzveranstaltung ausgesprochen. Der Vorstand hat in seiner Webkonferenz am 08.06. die Ergebnisse erfreut zur Kenntnis genommen und als Stärkung des Auftrags für die Organisation der Herbsttagung angenommen. Dass eventuelle Einschränkungen zum Infektionsschutz auch im September noch gelten, wird von der Mehrheit der Umfrageteilnehmer (73%) akzeptiert. Über 50% der Umfrageteilnehmer sind auch bereit, virtuelle Vorträge zu akzeptieren, allerdings votierten immerhin 35% stark für den Live Vortrag.

Nachruf Hartmuth Wehrs

In der Börsenwelt hätte man ihn als Blue Chip für das Marketing der Krankenhaus-IT beschrieben. - Hartmuth Wehrs, geboren am 11. März 1948, trat in mein persönliches, wie unser Verbandsleben, am 25. April 2002. Der Bundesverband der Krankenhaus-IT-Leiter war noch nicht gegründet, aber die Vorbereitungen liefen auf Hochtouren. Hartmuth Wehrs kam nach Konstanz zur Tagung und interviewte mich zu den Zielen der Arbeitsgemeinschaft der Krankenhaus-IT-Leiter. Ich würde es heute als eine Art Symbiose bezeichnen. Denn wir alle haben davon profitiert und uns erfolgreich weiterentwickeln können. Als Herausgeber der Fachzeitschrift „Das Krankenhaus-IT-Journal" begleitete Hartmuth Wehrs den KH-IT von Beginn an. Seit 2016 ist das Krankenhaus-IT Journal das offizielle Verbandsorgan des Bundesverbandes der Krankenhaus IT Leiterinnen und Leiter e.V. (KH-IT), quasi der Ritterschlag für seine Herausgeber Tätigkeit. Wir haben gemeinsam die Gelegenheiten zum gegenseitigen Austausch über das Gesundheitswesen und insbesondere die Krankenhaus IT bei Tagungen und Messen gepflegt.

Wir, die Menschen, die ihn kennenlernen durften, werden ihn im Herzen behalten und sein Andenken ehren. Sein Lebenswerk, unser Verbandsorgan, wird uns weiter auf dem Weg begleiten.

Dankbar nehmen wir Abschied von Hartmuth Wehrs.
15. Mai 2020

Heiko Ries
Ehrenvorsitzender des KH-IT, im Namen des Vorstandes und des gesamten Verbandes der Krankenhaus-IT-Leiter, KH-IT

Verbandstermine 2020

16.09.2020–17.09.2020 Herbsttagung im Universitätsklinikum in Münster: Anwenderperspektiven & Neuentwicklungen

Health-IT-Talk in Berlin-Brandenburg
13.07.2020 *Webinar: Terminologien in der Routine – Beispiele und Anwendungen*
10.08.2020 *Medizininformatik-Initiative Deutschland des BMBF - Update*

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.

TOGETHER FOR SUCCESS

Yesterday.
Today.
And from this day on.

Dedalus
HEALTHCARE SYSTEMS GROUP

www.dedalusgroup.de

"Nicht in alte Verhaltensmuster zurückfallen"

Die aktuelle Situation zeigt, wie wichtig eine effiziente Digitalisierung ist. Corona erweist sich als Digitalisierungsbooster in Krankenhäusern. Über die Auswirkungen auf die Krankenhäuser und die Führungskräfte sprach das Krankenhaus-IT Journal mit Oliver Heitz, Healthcare Consulting der Personalberatung Rochus Mummert.

Was hat sich im Zuge der Corona-Krise geändert und wie geht es nach der Krise weiter?

Diverse Faktoren – wie beispielsweise die Angst vor dem Neuen und Unbekannten oder Bedenken hinsichtlich des Datenschutzes – hatten vor der Krise einen enormen Einfluss auf die Realisierung von Digitalisierungsprojekten in Kliniken. In Krankenhäusern wurde zwar viel über diese Themen diskutiert, aber wenig ausprobiert bzw. umgesetzt. Hinzu kamen die fehlende Investition in Technologie und auch das mangelnde Wissen über passende technische Lösungen.

Die Krise brachte alle zum selben Zeitpunkt in die gleiche Ausgangslage: Um weiter funktionieren zu können, mussten überall von jetzt auf gleich Lösungen her. Der kurzfristige Lockdown ließ keine monatelangen Testphasen zu, wie man sie sonst gewohnt war. Es wurde sehr zügig über Anschaffungen entschieden und experimentiert, da den Häusern schlussendlich nichts anderes übrigblieb. Mit höchstem Engagement wurde auf die Schnelle eine digitale Infrastruktur geschaffen, die zum Erstaunen aller bis heute recht gut funktioniert. So haben die Kliniken die Bestätigung, dass beispielsweise Video-Konferenzen auch per Smartphone gelingen, Homeoffice per VPN-Tunnel hinreichend sicher ist, ein Smartphone auch ein guter Scanner ist und auf einem Touchscreen wunderbar unterschrieben werden kann.

Die Herausforderung ist nun, diesen Schwung mitzunehmen und nicht in alte Verhaltensmuster zurückzufallen. Wichtig hierbei ist, dass alle – von den Mitarbeitern über die Personalvertretungen bis hin zur Geschäftsführung – an einem Strang ziehen. Auch ausreichend investive Mittel müssen – bei aller finanzieller Knappheit – in die Hand genommen werden. Das jüngst verabschiedete Zukunftspaket der Bundesregierung sieht für Krankenhäuser eine Unterstützung von 3 Mrd. Euro vor. Runtergebrochen wären dies 1,6 Mio. EUR pro Krankenhaus bzw. 155 EUR pro Krankenhauspatient. Laut DKG (Stand: Dezember 2019) fehlen den Krankenhäusern allerdings insgesamt 30 Mrd. EUR. So gesehen würde die, von der Bundesregierungen geplante Summe lediglich 10% des tatsächlichen Bedarfs decken. Die zur Verfügung stehenden finanziellen Mittel könnten somit zu einem nicht zu unterschätzenden Hemmfaktor im Digitalisierungsprozess werden.

Oliver Heitz, Healthcare Consulting der Personalberatung Rochus Mummert

Was können und müssen Krankenhäuser aus der Krise lernen? Und was müsste nun möglichst vermieden werden?

Aus meiner persönlichen 25-jährigen Sicht auf deutsche Kliniken darf deren Projektmanagement noch effizienter werden. Es muss nicht immer gleich die perfekte Lösung

sein, oft führen bereits kleine Schritte in die richtige Richtung. Eine Krise ruft zu Entschlossenheit und Entscheidungsfreude auf, gleichzeitig werden Fehler aufgrund der großen Unsicherheit eher verziehen. All das sollten sich Führungskräfte bewahren und mit großer Dynamik weiter die IT-Projekte vorantreiben. Es gilt den Schwung mitzunehmen und die Motivation – auch im Sinne einer Begeisterung für die neue Technik – aufrechtzuerhalten.

Führungskräfte tragen eine große Verantwortung beim Digitalisierungsprozess. Wie sieht es derzeit mit ihren Digitalisierungskompetenzen aus und wie können diese erworben bzw. erweitert werden?

2018 haben wir bei Rochus Mummert eine Studie zum Thema Digitalisierung in der Gesundheitswirtschaft durchgeführt. 59% der Studienteilnehmer gaben an, dass im medizinischen Bereich Digitalisierungswissen zukünftig ein wichtiges Einstellungskriterium sein wird. Im Rahmen unserer Besetzungsprozesse – sei es bei administrativen aber eben auch bei medizinischen Positionen – schauen wir daher immer mehr auf die Digitalisierungskompetenz. Diese ist schwer zu erfassen, da es bisher kaum eine systematische Ausbildung oder Qualifikation hierzu gibt. Für mich ist es wichtig herauszufinden, ob ein verantwortlicher Mitarbeiter „digital denken" kann. Also schaue ich weniger auf das Gelernte, sondern auf die Anwendbarkeit in anderen Zusammenhängen. Mir geht es um die Transformation von digitalem Wissen. Also diskutiere ich mit Personen deren differenzierten Erfahrungen, Erwartungen beim neuen Arbeitgeber und Wunschvorstellungen an die Zukunft. Nach meiner Einschätzung erfolgt die Aneignung und Schärfung von Digitalisierungskompetenzen hauptsächlichen nach dem Prinzip „Learning by Doing" und ist ein stetiger Prozess. Wichtig sind zudem eine starke Selbstreflexion und die persönliche Auseinandersetzung mit dem erworbenen Wissen. Wenn man sich in diesen Entwicklungsprozess begibt, dann nimmt auch der Digitalisierungsgrad im eigenen Arbeitsumfeld fortlaufend zu.

Die Corona-Pandemie stellt alle Branchen vor extreme Herausforderungen. Was bedeutet das konkret für die Führungskräfte in Krankenhäusern? Wie kann ein virtuelles Management von Krankenhäusern gelingen?

Während der aktuellen Phase habe ich mich mit sehr vielen Führungskräften von Krankenhäusern unterschiedlicher Professionen und Hierarchien ausgetauscht. Alle bestätigten beispielsweise die Aussage, dass im letzten Jahr niemand ein breitflächiges Homeoffice für möglich gehalten hätte. Ebenso waren Online-Schulungen und Video-Konferenzen nur im Einzelfall eine Option. Das hat sich schlagartig geändert, was auch sehr gut ist. Bei aller Euphorie hierüber zeigt sich jetzt aber auch eine Kehrseite: Viele Führungskräfte sind mit der virtuellen Führung ungeübt und teilweise auch überfordert. Das zeigt sich in einer Überkontrolle, sodass Mitarbeiter viel intensiver kontaktiert werden als im Büro. An dieser Stelle müssen nun Führungskräfte intensiv auf die neue Arbeitsweise geschult werden. Andere Branchen sind Krankenhäusern da sehr weit voraus. In weltweit aufgestellten Konzernen sitzen selten alle Mitarbeiter im selben Land, in derselben Stadt, geschweige denn im selben Gebäude. Virtuelles Management ist eben nicht allein die Einführung einer elektronischen Stempeluhr auf dem Computer des Mitarbeiters. Vielmehr kommt es auf die klare Kommunikation zu Erwartungen und Zeitplänen an. Die Führungskraft muss sich mehr um die Rahmenbedingungen und Ressourcen kümmern, damit der Mitarbeiter seine Aufgabe erledigen kann. Hinzu kommen seitens der Führungskraft die Unterstützung im Sinne von Coaching und Motivation. Das alles ist auch gut mit digitalen Hilfsmitteln möglich und erfordert keine persönliche Anwesenheit. Es muss ein Umdenken stattfinden, das auch mehr Lockerheit und Vertrauen beinhaltet. Eine sehr große Herausforderung ist allerdings, die Teamzugehörigkeit über diverse Standorte hinweg aufrechtzuerhalten. Um das Zugehörigkeitsgefühl zu stärken, sollten beispielsweise ab und zu virtuelle Kaffeepausen eingelegt und anstelle von Telefonaten oder Mails auch mal spontan Video-Calls genutzt werden. Wackelige Handy-Videos verstoßen Dank Corona nicht mehr gegen den Business-Knigge.

Über den Gesprächspartner:

Im Bereich Healthcare Consulting der Personalberatung Rochus Mummert berät Oliver Heitz seit mehr als zehn Jahren bei der Besetzung von Spitzenpositionen im Gesundheitswesen. Er verbindet seinen Beratungsschwerpunkt mit der Besetzung von kaufmännischen, medizinischen und pflegerischen Fach- und Führungspositionen im Healthcare- und Life Science Bereich sowie Management-Audits, Entwicklung von Personalstrategien, Onboard-Coaching, Arbeitgeberattraktivität und kundenorientierte Reorganisation von Personalbereichen.

DRK Kliniken Berlin erreichen mit ORBIS Speech neue Stufe der Effektivität

Sprechen statt schreiben

Zeitdruck ist der stete Begleiter von Ärzten, ineffiziente Abläufe sind ein Ärgernis. Die DRK Kliniken Berlin treten dem entgegen und unterstützen die Mediziner mit der Spracherkennung ORBIS Speech. Das Ergebnis ist bereits nach wenigen Monaten überaus erfreulich.

Die DRK Kliniken Berlin expandieren ständig. Zu den heute bereits 27 Kompetenzzentren sollen kurzfristig weitere hinzukommen. Um bereichsübergreifend einen nahtlosen Datenaustausch zu gewährleisten, verfolgt die Einrichtung einen holistischen IT-Ansatz. „Wir setzen klinikweit in Medizin und Administration bereits seit 1997 einheitlich auf das Krankenhaus-Informationssystems ORBIS KIS und versuchen, dort so viele Prozesse wie möglich abzubilden", sagt Daniel Schmidt, Bereichsleiter Medizin- und Informationstechnologie, „und so auf einen Mix von Subsystemen zu verzichten."

Prozessunterstützung lautet seit jeher das oberste Gebot. Dazu haben die DRK Kliniken Berlin bereits 2007 eine erste Spracherkennungslösung mit digitalem Diktat eingeführt – außerhalb von ORBIS. „Allerdings haben uns die Anwender immer häufiger gefragt, ob es nicht eine ins KIS integrierte Lösung gibt", berichtet Tobias Knüppel, Leiter Klinische IT-Systeme. Das Handling sei mit der bestehenden Lösung zu aufwendig und vorhandene Formulare könnten nur eingeschränkt genutzt werden, waren die Hauptkritikpunkte. „Hinzu kam, dass die alte Lösung ob einer geringen Erkennungsrate auch nur von begrenztem Nutzen für die Ärzte war, worunter die Akzeptanz gelitten hat", führt Schmidt aus. Das führte dazu, dass zunehmend auf das gute alte Diktiergerät und den Schreibpool zurückgegriffen wurde. Also starteten Schmidt und seine Mitarbeiter die Suche nach einer tief ins KIS integrierten Spracherkennung, die nah an den definierten Prozessen arbeitet. „Mit ORBIS Speech haben wir dann einen Neuanfang gestartet, weil wir aus der Erfahrung bei meinem früheren Arbeitgeber sicher waren, dass die Lösung unsere hohen Ansprüche erfüllen kann", gibt Schmidt sich zuversichtlich.

Projekt mit Anlauf

Bereits 2018 war klar, dass die damals eingesetzte Spracherkennungssoftware nicht wirklich zielführend ist und geplante Weiterentwicklungen die DRK Kliniken in ihrem Wechselwunsch nicht umstimmen würden. Deshalb hat sich der IT-Bereich auf die Suche nach Alternativen begeben und aus besagten Gründen bei ORBIS Speech angeklopft. „Nach einer erfolgreichen Teststellung bei ausgewählten Radiologen, die uns durchweg positives Feedback gebracht hat, sind wir in die Gespräche mit der Geschäftsführung gegangen und konnten ORBIS Speech Ende vergangenen Jahres schließlich beschaffen", freut sich Schmidt.

Im Februar wurde als erste Einrichtung das Institut für interventionelle und diagnostische Radiologie am Standort Westend mit der neuen Spracherkennung ausgestattet. Anfang März startete der klinikweite Rollout. Alle Mediziner arbeiten mit dem integrierten Basiswortschatz für die Allgemeinmedizin. „Eine generelle Adaption ist vorerst nicht vorgesehen, da die Qualität der Erkennung deutlich höher ist als im Vorsystem", klärt Knüppel auf. „Selbstverständlich ergänzt jeder Anwender im Laufe der Arbeit seinen individuellen Wortschatz um spezielle Begrifflichkeiten und entwickelt ihn so weiter." Die IT führt diese Wortschätze dann für die gesamte Radiologie zusammen, so dass alle Ärzte Zugriff darauf haben. Das Trainieren des Wortschatzes ist sehr simpel und funktioniert live

Daniel Schmidt: „ORBIS Speech soll sich bereits nach einem Jahr amortisieren."

im System. „Der Arzt markiert ein falsch erkanntes Wort mit einem Sprachkommando, dann öffnet sich eine Maske, in die das Wort richtig eingegeben wird", beschreibt Knüppel den Ablauf.

Nach den radiologischen Instituten sind alle Abteilungen und Klinken in den Genuss der neuen Spracherkennung gekommen. „Das war und ist durchaus eine Herausforderung", sagt Schmidt, „weil die Prozesse unterschiedlich sind. Deshalb gilt es, die User jeder Abteilung an jedem Standort auf ORBIS Speech umzuschulen. Ziel ist es, dass nicht mehr der externe Schreibdienst für Arzt- und Entlassbriefe oder Befunde adressiert, sondern der gesamte Vorgang nur mithilfe der eigenen Sprache abgeschlossen wird."

Amortisation nach einem Jahr

Bis zum Jahresende 2020 sollen alle Fachbereiche und Abteilungen mit der Spracherkennung ausgestattet sein. Gelingt das, soll sich das gesamte Projekt – auch durch die unternehmensweite Zurückführung des Schreibdienstes – bereits im Jahr darauf amortisieren. Voraussetzung ist jedoch, dass es gelingt, die Diktatfunktion nur noch in Ausnahmefällen, etwa für schnelle Notizen in den Sekretariaten oder OP-Berichten, zu nutzen.

Potenzial für Einsparungen sind für Schmidt ausreichend: „Nach der Basisdokumentation werden wir weitere Prozesse und Dokumentationen, die in ORBIS erfolgen, über die Spracherkennung abbilden, angefangen bei OP-Berichten und der Pflegedokumentation bis hin zu umfangreichen Texten in der Psychiatrie." Die DRK Kliniken wollen ihre Lizenzen nicht nur an Ärzte vergeben, sondern auch an Verwaltungsangestellte, um beispielsweise Geschäftsbriefe zu schreiben.

Beim Rollout profitiert die IT von der Client-Server-Architektur. Die Engine von ORBIS Speech wird zentral auf einem Applikationsserver betrieben – inklusive aller Treiber und Konnektivität der Peripherie, also der Spracherkennungsmikrofone. „Damit erschöpft sich unser Aufwand auf das Anschließen der Mikrofone", so Knüppel. Die Serverressourcen sind so ausgelegt, dass sie einen stabilen Betrieb auch dann gewährleisten, wenn alle 400 Nutzer gleichzeitig auf das System zugreifen sollten. „Trotzdem behalten wir uns die Option des Load Balancing, also einer Lastverteilung, noch vor, sollten wider Erwarten Probleme auftreten", stellt der Leiter Klinische IT-Systeme klar.

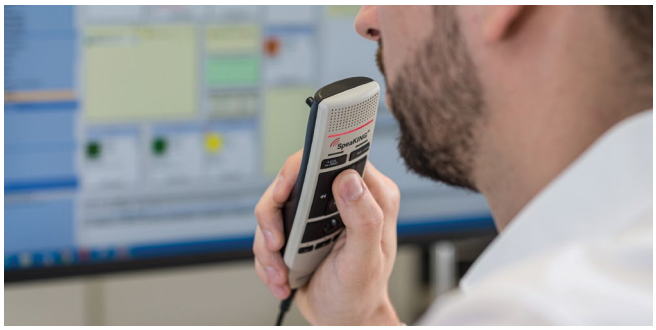
Zufriedenheit übertrifft Erwartungen

Genug der Theorie. Wie funktioniert ORBIS Speech nun in der Praxis? Der Radiologe öffnet seinen Fall mit allen Patientendaten und den Röntgenaufnahmen über die Arbeitsliste im RIS. Dann navigiert er mit einem Sprachkommando in das Befundfeld und kann den Text diktieren. Ist er fertig, kontrolliert er den Befund, nimmt gegebenenfalls Änderungen vor und vidiert ihn. Dadurch wird er gleichzeitig signiert und steht den Stationen über ORBIS KIS, wo der Befund automatisch abgelegt wird, zum Abruf zur Verfügung.

Im Entlassprozess werden die Dokumente geöffnet, Teile übernommen und so der Entlassbrief für den Haus- oder weiterbehandelnden Arzt diktiert. „Um diesen Prozess derart integriert abzubilden, ist eben eine tiefe Einbindung der Spracherkennung in die entsprechenden Systeme unerlässlich. „Sowohl bei Befunden als auch bei Arztbriefen ist es uns wichtig, dass die Ärzte die Felder ansprechen können. Solche Möglichkeiten sind in ORBIS Gold wert, weil wir den Anwendern damit ein System an die Hand geben, das sehr wenige manuelle Eingriffe erfordert und doch voll flexibel ist", streicht Knüppel einen wesentlichen Vorteil heraus.

Dabei bleibt es jedoch nicht, wie Schmidt ausführt: „Die Spracherkennung unterstützt die Arbeitsabläufe auf den Stationen und in den Funktionsbereichen massiv. Es gibt wenige Nacharbeiten, und es treten nur wenige Fehler auf. Ein solch reibungsloses System zur Unterstützung seiner Arbeit wünscht sich wohl jeder Anwender."

Dementsprechend hoch sind auch die Akzeptanz und Zufriedenheit bei den Ärzten. „Wir haben Mails bekommen, in denen sich die Mitarbeiter für die tolle Technologie bedankt haben", schmunzelt Tobias Knüppel. „Die Resonanz ist sehr positiv."



Die Spracherkennung ORBIS Speech gewährleistet eine schnelle Befundung und schnelle Abläufe.

Tobias Knüppel: „ORBIS Speech erfordert kaum manuelle Eingriffe und ist doch voll flexibel."

Weshalb Corona das Gesundheitswesen auch digital ans Limit bringt

Die digitale Transformation konfrontiert Ärzte, Kliniken und Pharmahersteller gleichermaßen mit neuen Herausforderungen. Waren Patientendaten früher noch in analoger Form als Akte oder Karteikarte archiviert, gilt es heutzutage, die digitalisierten Informationen vor unberechtigtem Zugriff zu schützen.

Neue medizinische Teilbereiche wie die Ferndiagnostik oder Implantate für Home Monitoring erfordern zudem eine sichere und verlässliche digitale Verbindung zwischen Ärzten und Patienten. Störungen, Ausfälle oder Manipulationen gefährden hier direkt die Gesundheit des Einzelnen. Ein drohender Infarkt, der von einem Herzschrittmacher mit Diagnose-Funktionalität normalerweise sofort gemeldet würde, bleibt bei einem Ausfall der Technik vorerst unerkannt.

Das Gesundheitswesen muss daher wie keine andere Branche seine IT-Systeme auf Sicherheit und Stabilität abstimmen. Nicht zuletzt aufgrund der Gefährdung von Leib und Leben zählt die Bundesregierung den Healthcare-Sektor zu den Kritischen Infrastrukturen (KRITIS), die besonders hohe Anforderungen an IT-Sicherheit erfüllen müssen und bei Vorfällen meldepflichtig sind.

Belastungsprobe COVID-19

Die derzeitige Corona-Pandemie stellt das globale Gesundheitswesen vor bisher nicht dagewesene Herausforderungen. In vielen Teilen der Welt gelangen Ärzte und Kliniken wegen der schieren Anzahl an Patienten an ihre Kapazitäts- und Belastungsgrenzen. Um diese Notsituation zu meistern, ist ein reibungsloser Betrieb – digital wie analog – unbedingt erforderlich.

Diese Notlage nutzen Cyberkriminelle gezielt aus. Nie war die IT-Infrastruktur von Praxen und Kliniken verwundbarer als jetzt. Im März kam es etwa zu professionellen Angriffen auf die Weltgesundheitsorganisation (WHO) - glücklicherweise waren die Cyberkriminellen nicht erfolgreich. Auch Angriffe auf Krankenhäuser haben sich in den letzten Wochen gehäuft. Phishing, Social Engineering und mit Schadcode versehene Corona-Informationsseiten kommen hinzu.

Fakt ist: Kein voll ausgelastetes Krankenhaus kann eine schwere Cyberattacke ohne schwere Verluste wegstecken. Die derzeitige Situation macht Betreiber und Entscheider besonders für Lösegeldforderungen anfällig, bei denen Angreifer dringend erforderliche Behandlungsdaten in digitale Geiselhaft nehmen. Digitale Attacken stellen damit eine ganz reale Gefahr für die Gesundheit der Patienten dar.

Kliniken und Arzt-Praxen im Visier von Cyberkriminellen

Zu den gängigsten Angriffsvektoren der Cyberkriminellen auf medizinische Infrastruktur zählen unter anderem DDoS-Attacken (Distributed Denial of Service). Diese Angriffe zielen auf die Nichtverfügbarkeit eines Servers oder Dienstes ab, indem eine Unmenge künstlicher Anfragen aus Botnetzen die betreffende Hardware lahmgelegt. Kritische Internet-Dienste, wie etwa die zentralen Informationsportale der Gesundheitsbehörden, welche die Bevölkerung über die aktuelle Notlage informieren, werden mittels DDoS von außen gezielt sabotiert. Ein ebenfalls sehr gängiges Angriffsmuster stellen Attacken mit Ransomware dar. Diese Erpressungstrojaner verschlüsseln selbständig Datensätze im Netzwerk und machen die darin enthaltenen Informationen dadurch unzugänglich. Um wieder an die Daten zu gelangen, werden die betroffenen Einrichtungen zur Zahlung von Lösegeldern gedrängt. In der Vergangenheit kam es schon mehrfach zu schweren Ransomware-Attacken auf Kliniken und Arztpraxen. Dieser Trend setzt sich in der Corona-Krise leider verstärkt fort. Verschlüsselungstrojaner können im Ernstfall Menschenleben kosten und verursachen Millionenschäden. Es dauert oft Wochen oder Monate, bis sämtliche Systeme einer betroffenen Klinik wieder ans Netz zu bringen. Gerade jetzt ist das ein beängstigendes Szenario.

Derzeit noch weniger verbreitet, aber potenziell mit schweren Konsequenzen behaftet ist die gezielte Manipulation kritischer Gesundheitsdaten. Durch die zunehmende Vernetzung von Monitoring-Geräten und die Einbeziehung von Gesundheitstrackern und Wearables in die Behandlung von Patienten vergrößert sich die virtuelle Angriffsfläche exponentiell. Sicherheitslücken in Schnittstellen oder Geräte-Firmwares bieten Angreifern hier die Möglichkeit, generierte Datensätze zu verfälschen. Die manipulierten Informationen können wiederum zu Fehldiagnosen oder Fehlmedikationen führen. Um diesen Angriffsvektor zukünftig abzuwehren, muss massiv in die IT-Sicherheit dieser Geräte investiert werden.

Gesundheitswesen erfordert ganzheitliche Sicherheit

Alle drei beschriebenen Bedrohungsszenarien stellen für Ärzte und Kliniken bereits im normalen Betrieb eine Herausforderung dar. Zu Zeiten der Corona-Pandemie sind solche Ausfälle dagegen oftmals lebensbedrohlich.

Nicht umsonst greifen für das Gesundheitswesen strenge regulatorische Vorschriften für Cybersicherheit und Datenschutz. Während etwa die europäische Datenschutz-Grundverordnung (DSGVO) auf den Schutz sensibler Patientendaten abzielt, regelt das besonders für KRITIS-Betreiber relevante IT-Sicherheitsgesetz die Absicherung digitaler Systeme. So müssen etwa mitunter die digitalen Krankenhausinformationssysteme (KIS) in Kliniken redundant über Notfallpläne abgesichert sein, damit wichtige Patienten- und Behandlungsdaten auch bei Ausfällen oder Angriffen zugänglich sind. KRITIS-Einrichtungen haben zudem regelmäßig nachzuweisen, sämtliche verfügbaren Mittel, die zum Schutz ihrer Systeme erforderlich sind, einzusetzen.

Professionelle Schutzlösungen für den Healthcare-Bereich

Im Fall der oben beschriebenen Angriffsvektoren umfasst dies etwa einen hochspezialisierten DDoS-Schutz, der genau diese Art von Attacken adressiert. Professionelle Schutzanbieter sind dazu in der Lage, Webseiten und Online-Dienste in Echtzeit zu analysieren und den schädlichen Traffic zu diagnostizieren. Der bösartige Datenverkehr wird dann herausgefiltert, damit die Serverkapazitäten allein den validen Nutzeranfragen zur Verfügung stehen.

Zur Abwehr von Ransomware ist vor allem eine Sensibilisierung des Personals erforderlich. Zumeist gelangt die Schadsoftware über Phishing- oder Spam-E-Mails in die Netzwerke von Kliniken und Arztpraxen. Regelmäßige Awareness-Schulungen und Trainings bereiten Mitarbeiter auf den Umgang mit diesen Gefahren vor – gelegentliche Stichproben (etwa über Phishing-Test-Mails) geben Aufschluss darüber, ob die Mitarbeiter die Verhaltensregeln auch beherzigen.

Daneben gelten natürlich auch für Krankenhäuser die üblichen Best-Practise-Methoden der Cybersicherheit. So sollten etwa stets alle Systeme auf dem aktuellen Stand gehalten und zeitnah mit verfügbaren Sicherheitsupdates versorgt werden. Auch das regelmäßige Anlegen von Backups kritischer Datensätze zählt zu den gängigen Standards.

Wer die gängigen Vorgaben für eine ganzheitliche Sicherheitsstrategie erfüllt, dessen Systeme sind auch in Notsituationen der gestiegenen Belastung gewachsen. Gerade in der Corona-Krise ist es daher essenziell, dass trotz Überlastung und Stress in den Kliniken die IT-Sicherheit ganz oben auf der Agenda steht, um digitale Angriffe erfolgreich abzuwehren. Wir denken, dass die IT-Abteilung der Klinik heutzutage genauso wichtig ist wie die Intensivstation.

Zum Autor

Paul Kaffsack ist Geschäftsführer des deutschen Technologieherstellers Myra Security. Er ist seit 20 Jahren in der digitalen Welt aktiv und ein gefragter Experte auf internationalen Konferenzen. Als IT-Sicherheitsunternehmen bietet Myra eine zuverlässige, zertifizierte Security-as-a-Service Plattform zum Schutz digitaler Prozesse. Die smarte Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic, noch bevor virtuelle Angriffe einen realen Schaden anrichten. Auf die Lösungen von Myra vertrauen unter anderem das Bundesministerium für Gesundheit (BMG), die Bundeszentrale für gesundheitliche Aufklärung (BZgA), die Bundesregierung sowie Banken und Versicherungen.

Digitalisierung für mehr Effizienz in der Versorgung

Durch die Digitalisierung von Prozessen sowie dem Erfassen, Auswerten und zielgerichtete Nutzen von Versorgungs- und Prozessdaten kann es Krankenhäusern zukünftig gelingen ihre Patientenversorgung wirtschaftlicher zu gestalten und wettbewerbsfähig zu bleiben. Gerrit Schick, Head of Healthcare Informatics, Philips GmbH Market DACH, beschreibt im Interview wie sich das Krankenhaus der Zukunft nach innen und außen vernetzen sollte, um seiner zentralen Rolle in der Patientenversorgung gerecht zu werden.

Wie bereit sind denn die Krankenhäuser für eine digitale Vernetzung?

Das kann so pauschal nicht beantwortet werden, denn die Bandbreite reicht von „alles bereit" bis zu Häusern, die noch am Anfang eines längeren Prozesses stehen. Es kommt darauf an wie sehr diese Häuser in den letzten Jahren ihre Infrastruktur für diese Vernetzung vorbereitet haben. Neben fehlenden investiven Mitteln kommt, dass es häufig auch keine klare Strategie und Zielarchitektur gab, so dass der entstandene Flickenteppich an IT Lösungen keine gute Ausganssituation für die erforderliche integrierte und vernetzte Lösung darstellt. Da sind Anbieter wie Philips, die konsequent auf offene, standardbasierte und interoperable Lösungen setzen sicherlich ein idealer Partner: denn diese Lösungen sind nicht nur leicht integrierbar und für Vernetzung bereits vorbereitet, darüber hinaus bieten wir auch Technologien an um die Interoperabilität für andere, existierende IT Systeme herzustellen und damit eine Gesamtlösung für die Häuser aus einer Hand bereitstellen zu können.

Und wie wird der Patient in diese Vernetzung mit eingebunden?

Auch hierfür gibt es spezielle Lösungen wie unsere Vital-Health Plattform: Die Module Online-Terminbuchung, Terminvor- und -nachbereitung, Nachsorge/eTherapy und Qualitätsmanagement können zunächst einzeln in die Infrastruktur eines Krankenhauses itegriert werden. Jedes Modul verfügt über die erforderlichen offenen Schnittstellen, unterstützt Interoperabilitätsstandards und kann problemlos auch in bereits vorhandene IT-Systeme anderer Anbieter eingebettet werden. Bei Philips werden auf offenen Standards beruhende Schnittstellen wie DICOM, IHE, HL7 Nachrichten und HL7 FHIR zur Gewährleistung des Datentransfers verwendet. Dasselbe gilt auch für die Gesamtlösung, die dann auch noch den Vorteil der einheitlichen Nutzererfahrung mit sich bringt.

Wer profitiert am meisten von der Vernetzung durch Digitalisierung?

Die Vorteile einer Digitalisierung lassen sich erst vollständig ausschöpfen, wenn die Vernetzung sowohl intersektoral als auch an Sektorenübergängen geschaffen wird. Nur durch den so entstehenden permanenten Informationsaustausch lässt sich die Behandlungsqualität steigern und auch die Ergebnisqualität der gesamten Versorgungskette evaluieren. Am Ende dient sie primär zum Wohle des Patienten.

Gerrit Schick, Head of Healthcare Informatics, Philips GmbH Market DACH

synedra AIM für RHÖN-KLINIKUM Campus Bad Neustadt

Health Content Management auf höchstem Niveau

Am RHÖN-KLINIKUM Campus Bad Neustadt wurden nicht nur insgesamt fünf Kliniken in einen gemeinsamen Campus überführt, sondern auch die IT-Landschaft der unterschiedlichen Einrichtungen konsolidiert. Eine wichtige Rolle bei der hochmodernen IT-Infrastruktur am Campus spielt die Health Content Management Plattform synedra AIM des IT-Unternehmens synedra, die als digitales Universalarchiv den Zugriff auf alle medizinischen Daten am Campus ermöglicht.

Seit Ende 2018 vereinigt der Campus Bad Neustadt, einer von fünf Standorten der RHÖN-KLINIKUM AG, fünf Kliniken auf einem Areal. Ziel des Neubau- und Konsolidierungsprojekts war es, die verschiedenen Kliniken, Rehabilitationseinrichtungen und das Medizinische Versorgungszentrum am Standort Bad Neustadt zusammenzufassen und organisatorisch neu zu gruppieren. Im Zuge dieser Neuaufstellung wurde auch eine Neuausrichtung der IT-Landschaft notwendig. Eine der größten Herausforderungen beim Umzug auf den Campus stellte aus Sicht der IT die Zusammenführung der unterschiedlichen Krankenhaus-Informationssysteme in ein einheitliches KIS für den gesamten Campus dar. Um dieser Herausforderung zu begegnen, entschied man sich für eine Zusammenarbeit mit dem in Österreich ansässigen IT-Unternehmen synedra. Rund 6,5 Millionen Dokumente wurden zu Projektbeginn aus den Krankenhaus-Informationssystemen der fünf Kliniken in synedra AIM migriert.

Ein Archiv für alle Daten

„Der nächste Schritt bestand darin, eine enge Integration zwischen dem Universalarchiv von synedra und dem führenden Informationssystem, dem KIS iMedOne® der Deutsche Telekom Clinical Solutions GmbH (DTCS), zu realisieren", erläutert Gernot Enzenberg, Projektleiter seitens synedra, das weitere Vorgehen. „Dafür haben wir auf Seiten des Universalarchivs den zugehörigen Endpunkt des Archivkonnektors – ein von der DTCS entwickeltes bidirektionales Archivierungsprotokoll – implementiert, mit dem es möglich ist, Dokumente aus dem iMedOne® zur Archivierung zu empfangen und umgekehrt Dokumente, die in synedra AIM durch Importvorgänge entstehen, durch einen Verweis im iMedOne® zu registrieren."

Doch nicht nur die Daten aus dem KIS, sondern alle am Standort generierten Daten sollten im Universalarchiv konsolidiert werden. „Unser Ziel war es, das digitale Archiv zur Eröffnung des neuen Campus aus dem klinischen System aufrufen zu können, idealerweise auch auf dem iPad im Rahmen der mobilen Visite", unterstreicht Konstanze Freisinger, Leiterin Klinische Systeme Konzern-IT. Dafür wurde zunächst die Viewing-Lösung synedra View Embedded in iMedOne integriert. Die Ärztinnen und Ärzte am Campus können nun auf Befund- und Bilddaten zugreifen, ohne dabei die KIS-Applikation verlassen zu müssen. „Dank synedra können wir ein systematisch gut sortiertes Archiv nutzen, welches uns auf jedem Computerarbeitsplatz der Klinik zur Verfügung steht. Zügig und zuverlässig können wir relevante Informationen unserer Patienten nachschlagen", fasst Dr. Bernd Kolbe, Oberarzt an der Klinik für Fuß- und Sprunggelenkchirurgie, die Vorzüge des neuen Universalarchivs zusammen. Eine weitere Anbindung zwischen der mobilen Viewing-Lösung synedra Web und der iMedOne iOS App bringt den Ärztinnen und Ärzten den zusätzlichen Nutzen, dass sie auch während der mobilen Visite über die iMedOne App auf dem iPad die Daten aus synedra AIM aufrufen und betrachten können.

Integration von Fremdsystemen

„Mit synedra AIM haben wir uns eine Lösung ins Haus geholt, die bei der Anbindung von Fremdsystemen sehr flexibel ist", freut sich Dr. Tobias Müller über die Entscheidung für synedra als Projektpartner. So greift beispielsweise das Medical Cockpit von Mindbreeze als konsumierendes System über REST-API auf synedra AIM zu. Als produzierendes System nennt der Leiter der Stabsstelle Digitale Transformation die zentrale Scanstrecke am Campus, bei der von Patienten mitgebrachte Unterlagen eingescannt und über den synedra-eigenen Importprozess in das Archiv überführt werden.

Weitere Ausbauschritte: PACS-Ablösung

Im Herbst 2019 entschied man sich am Campus Bad Neustadt dafür, das bis dahin im Einsatz befindliche PACS ebenfalls durch synedra AIM zu ersetzen. „Bereits im Januar 2020", so Tobias Juen, Projektleiter seitens synedra für das PACS-Projekt, „konnte die produktive Nutzung von synedra AIM als PACS in der Radiologie gestartet werden." In der sehr kurzen Projektdauer wurden 30 Befundworkstations und 70 Betrachtungsworkstations mit dem Bildbetrachtungs- und Befundungs-Tool synedra View ausgestattet. Die Abbildung der Teleradiologie sowie die Anbindung einer Vielzahl von Geräten – angefangen bei konventionellen Röntgengeräten über CT und MRT bis hin zu DSA und Ultraschall – stellen einen zentralen Mehrwert der neuen PACS-Lösung dar.

Positive Bilanz von allen Seiten

„Die Zusammenarbeit mit synedra kann ich als durchwegs positiv beschreiben. Der Support und die Projektarbeit haben sehr gut funktioniert", fasst Frithjof Eckhardt, Projektleiter bei der Umsetzung des Universalarchivs am Campus, seine Eindrücke zusammen. Auch hinsichtlich der PACS-Einführung zeigen sich beide Projektpartner zufrieden. „Die Radiologen sind begeistert von der Geschwindigkeit des neuen PACS. Daneben sind sie über den Funktionsumfang und die Tatsache, dass synedra AIM voll integrativ mit iMedOne verknüpft ist, sehr erfreut", weiß Dirk van Velsen, Projektleiter bei der PACS-Einführung am Campus, zu berichten. „Der vollumfängliche Ausbau von synedra AIM zu einer Health Content Management Plattform unterstreicht das Potential der Lösung und zeigt zugleich die möglichen Einsparpotentiale in der IT-Systemlandschaft von Krankenhäusern auf. Wir freuen uns, dass wir zusammen mit dem Campus Bad Neustadt ein PACS-Projekt realisieren konnten, das für die synedra Deutschland GmbH einen wichtigen Meilenstein im deutschen Markt darstellt", zieht Klaus-Philip Baldin, Leiter des synedra Hauptstadtbüros Berlin, positive Bilanz.

Wie IT-Profis mit intrinsischer Security kritische Infrastrukturen sicherer machen

Die Helden des IT-Klinikalltags

Die aktuelle Situation führt uns überdeutlich vor Augen, auf was es im Leben ankommt: Gesundheit und die damit verbundene Sicherheit des menschlichen Lebens sind das A und O. Andere wichtige Werte wie Freiheit und die Verwirklichung unserer Träume lassen sich nur dann umsetzen, wenn wir gesund sind. Ärzte, Pflegekräfte, Mediziner leisten gerade Unglaubliches. Sie retten Leben und setzen dabei mitunter ihr eigenes Leben auf's Spiel. Sie werden zurecht beklatscht. Doch ebenso viel Applaus verdienen diejenigen, die auf der medizinischen Bühne nicht so präsent sind, aber dafür Sorge tragen, dass der klinische Betrieb auch in diesen schwierigen Zeiten am Laufen gehalten wird. Es sind die stillen Helden des Klinik-Alltags, die – oftmals verborgen in Keller- oder Hinterräumen – 24-Stunden-Schichten fahren, an Wochenenden und Feiertagen nicht bei ihren Familien sind, um sicherzustellen, dass die systemkritischen Systeme in Kliniken und Notfallambulanzen reibungslos funktionieren: die IT-Helden stellen sicher, dass kein wichtiger Krankenhaus-Server ausfällt, dass das Krankenhauspersonal dank mobiler Technologien flexibler und näher am Patienten arbeiten kann und dadurch genug Zeit für die wichtigen Dinge bleibt. Die IT ist das Rückgrat der Krankenhäuser – und steht doch seit vielen Jahren unter einem enormen Kostendruck.

Dabei sind gerade Organisationen aus dem Gesundheitswesen häufiger Angriffen auf ihre IT-Umgebungen ausgesetzt als das in anderen Branchen der Fall ist. Cyberangriffe sind für das Gesundheitswesen ein sehr ernstzunehmendes Problem. Im Rahmen einer VMware-Studie gaben zwei von fünf befragten Healthcare-Vertretern an, dass ihre Organisation schon einmal einem Cyberangriff zum Opfer gefallen ist. Die gute Nachricht ist: Um die Qualität der Patientenversorgung zu verbessern und dabei auch die größtmöglichen Sicherheitsstandards umzusetzen, bedarf es nicht zwangsweise neuer Produkte, sondern vielmehr eines strategischen Neuansatz, was das Security-Konzept anbelangt.

Intrinsische Security ist die Zukunft der IT-Sicherheit

Denn traditionelle Hardware-basierte Konzepte bieten Kliniken nicht die benötigte Sicherheit, die aufgrund der Komplexität der Herausforderungen erforderlich ist. Unumgänglich ist vielmehr ein Software-basierter Ansatz, der Intrinsic Security beinhaltet, ein Beispiel hierfür ist die Plattform für Netzwerkvirtualisierung VMware NSX. Dazu werden Sicherheitskomponenten in die bestehenden Netzwerk- und Sicherheitslösungen integriert. Anders als früher, wo nur das gesamte System nach außen mithilfe einer Firewall abgesichert wurde, erfolgt inzwischen eine Absicherung auf Workload-Level. Auf jedem Workload befindet sich eine spezielle Firewall im Rahmen der Mikrosegmentierung. Dabei wird das Netzwerk in verschiedene Schutzklassen unterteilt: Neben besonders schützenswerten Patientendaten, die von außen nicht zugänglich sind, gibt es zusätzlich Schutzklassen mit mittlerem Schutzbedarf, für Verwaltungsdaten oder Abrechnungen. Hinzu kommt ein spezielles Segment für medizinische IT-Geräte, das Angreifer hindert ins Netzwerk zu gelangen. So wird ein optimaler, granularer Schutz erreicht.

Aktivieren von Firewalls, unabhängig vom Bereitstellungsort der Workloads

Anstelle von mehreren komplexen, teuren und nachgerüsteten Sicherheitsarchitekturen bietet VMware damit einen völlig neuen Sicherheitsansatz. Die in den Hypervisor integrierte VMware Service-Defined Firewall, die auf jedem Host verfügbar ist, merzt mögliche Schwachstellen aus, ist Workload-orientiert und vermeidet eine Störung des Datenflusses. Indem IT-Professionals den gesamten Sicherheits-Stack in der Krankenhaus-IT virtualisieren, profitieren sie von einem umfassenden, integrierten Infrastrukturschutz. Das ermöglicht ihnen eine Vorreiterrolle im Vergleich zu herkömmlichen Infrastrukturen – und macht sie zu den IT-Helden des Klinikalltags.

Wollen Sie mehr zum Aufbau sicherer Infrastrukturen und zum integrierten Security-Konzept von VMware erfahren? Die VMware-Healthcare-Experten stehen Ihnen mit Rat und Tat zur Seite – virtuell, auf Abstand und gerne auch immer persönlich!

Carsten Kramschneider
Manager, Solution Engineering – Public / Healthcare und Commercial, Deutschland, VMware

Kritische Infrastrukturen im Fokus – Handlungsempfehlung und Intrinsic Security für Krankenhäuser

Was kritische Infrastrukturen im Gesundheitswesen jetzt tun sollten, damit die IT für die aktuellen Anforderungen gerüstet ist: In Zeiten einer Pandemie sind Krankenhäuser die vorderste Front und damit extrem unter Druck. Steigende Patientenzahlen, schwere Krankheitsverläufe, krankheitsbedingte Ausfälle beim Personal, schneller Aufbau von neuen Stationen, Geräten und Krankenhausbetten. Dies alles setzt auch die Krankenhaus-IT unter Druck, die jetzt schnell, unkompliziert und unbürokratisch handeln sollte, um das medizinische Personal so gut wie möglich zu unterstützen.

Gut aufgestellt sind Kliniken, die bereits auf eine moderne IT-Infrastruktur setzen und fortgeschritten bei der digitalen Transformation sind. Im Rechenzentrum ist eine Software-definierte Architektur der richtige Weg, um IT-Services flexibel hinzuzufügen und einfach zu verwalten. Die schnelle Bereitstellung neuer Infrastrukturen kann über Cloud-Service-Modelle realisiert werden. Laut KRITIS werden Krankenhäuser mit über 30.000 stationären Fällen als Betreiber kritischer Infrastrukturen eingestuft und gelten damit als besonders schützenswert. VMware hat eine Handlungsempfehlung für kritische Infrastrukturen nach dem branchenspezifischen Sicherheitsstandard BS3 entwickelt, die Bereiche wie Netz- und Systemmanagement, Härtung und sichere Basiskonfiguration der Systeme und Anwendungen, Schutz vor Schadsoftware, Intrusion Detection / Prevention sowie sichere Authentisierung und weitere umfasst. Dieser Leitfaden gibt Krankenhaus CIOs Empfehlungen an die Hand, wie sie ihre Organisation absichern und Sicherheitsstandards einhalten.

Sicherheitsstandards auch wichtig für kleinere Krankenhäuser

Kleinere Krankenhäuser und Einrichtungen werden aktuell nicht zu den kritischen Infrastrukturen gezählt, für die solch strenge Sicherheitsregularien greifen. Allerdings sollten sich auch kleinere Einrichtungen an diesen Vorgaben orientieren, um keinen Ausfall ihrer IT-Systeme zu riskieren. Denn sensible Patientendaten sind unabhängig von der Größe der Einrichtung als besonders schützenswert einzustufen. Zumal in ländlichen Gebieten nicht immer große Einrichtungen vorhanden sind. Kommt es dort zu einem Cyberangriff, kann es in einer ganzen Region zu einem medizinischen Engpass kommen.

Intrinsic Security: ein Konzept für sichere Infrastrukturen und Medizingeräte

Ein sensibler Bereich innerhalb kritischer Infrastrukturen sind Medizingeräte, wie CT, Röntgen-, Ultraschall- oder Beatmungsgeräte. Diese sind heute meistens in irgendeiner Weise mit dem Internet verbunden. Medizinische IT-Geräte kommunizieren mit externen Wartungsservern der Hersteller, auf die die Krankenhäuser in der Regel keinen Zugriff haben. Darunter fallen Tablets, die Ärzte und Pflegepersonal bei der Visite einsetzen, ebenso wie elektronische Untersuchungsgeräte oder Navigations- und Planungssysteme für Operationen. Diese komplexen Systeme, die mit vielen weiteren technischen Komponenten im Krankenhaus abgestimmt werden müssen, sind mitunter nur sehr rudimentär abgesichert. Diese Schwäche können Hacker als Einfallstor zum gesamten Krankenhaus-Netzwerk nutzen.

Abhilfe schafft hier das Konzept der ‚Intrinsic-Security', einem ganzheitlichen End-to-End-Ansatz, das auf Mikrosegmentierung basiert. Durch den End-to-End-Ansatz wird durchgehende Sicherheit vom Datensatz bis zum Endgerät gewährleistet. Dabei wird durch die Segmentierung das Netzwerk in verschiedene Schutzklassen unterteilt: Neben besonders schützenswerten Patientendaten, die von außen nicht zugänglich sind, gibt es zusätzlich Schutzklassen mit mittlerem Schutzbedarf, für Verwaltungsdaten oder Abrechnungen. Die weniger kritischen Segmente sind beispielsweise das Entertainment-System in Patientenzimmern. Hinzu kommt ein spezielles Segment für Medizin-IT-Geräte, das Angreifer hindert ins Netzwerk zu gelangen.

Beim Aufbau sicherer Infrastrukturen und Schutz medizinischer IT-Geräte sollten Krankenhäuser auf bewährte Konzepte und zuverlässige Partner setzen, die viel Erfahrung im Gesundheitswesen mit sich bringen. Die Sicherheit und Zuverlässigkeit kritischer Infrastrukturen im Gesundheitswesen ist für die Gesellschaft überlebenswichtig – gerade in schwierigen Zeiten wie heute.

Carsten Kramschneider ist seit April 2015 verantwortlich für den Bereich Healthcare bei VMware. In dieser Position ist er für die Erschließung der vertikalen Märkte Gesundheitswesen und Health Insurance verantwortlich. Ziel ist es den Gesundheitsmarkt vom Leistungserbringer bis hin zum Kostenträger mit den Lösungen von VMware in den Bereichen Software-Defined Datacenter (SDDC), Security, Multi Cloud und End-User Computing bei der digitalen Transformation zu unterstützen.

Kommunikationstechnik im Pandemiefall: flexibel, robust und infektionssicher

SARS-CoV-2

Während die Krankenhäuser zum Normalbetrieb zurückkehren, bleibt die Gefahr einer zweiten Covid-19-Welle. Das neue Virus ist nicht zuletzt eine Herausforderung für die IT- und Kommunikationsinfrastruktur: Sie muss bei Bedarf schnell expandieren und die begrenzten Personalressourcen optimal nutzen – ohne dabei selbst zum Infektionsrisiko zu werden.

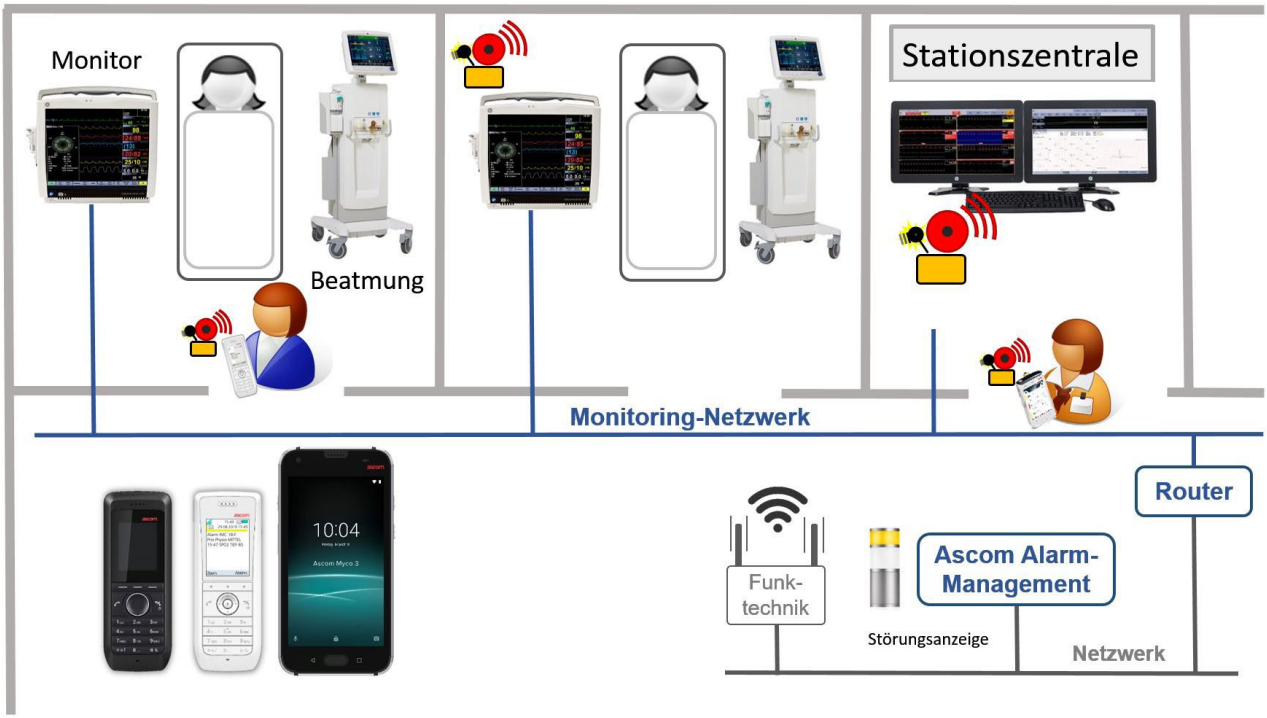
Von Dr. Udo Jendrysiak

Kliniken, und damit auch ihre IT-Abteilungen, stehen aktuell vor komplexen Organisationsaufgaben: Sie müssen zum geregelten Betrieb zurückkehren, wozu auch das Nachholen aufgeschobener Operationen zählt. Ein wiederaufflammendes Infektionsgeschehen könnte aber binnen weniger Wochen wieder eine Kehrtwende zum Krisenmodus erforderlich machen, sogar mit Hilfskrankenhäusern und zusätzlichen Notaufnahmeeinrichtungen.

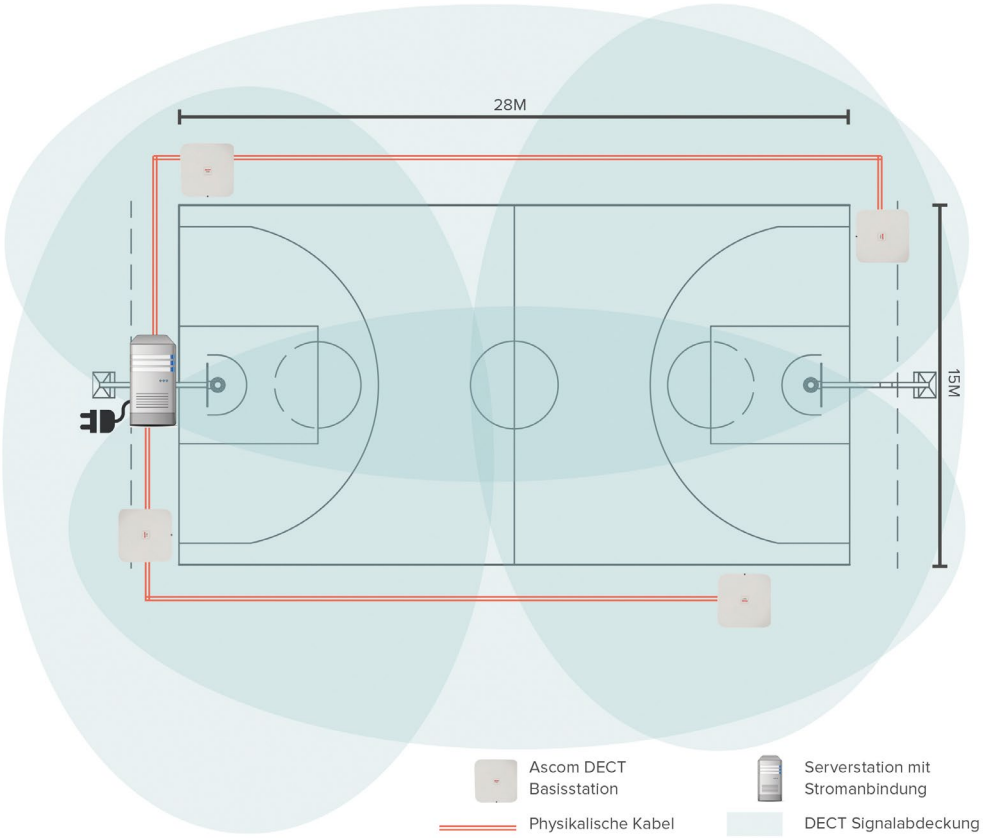
Dann wird nicht zuletzt bei der Kommunikationstechnik einiges improvisiert werden müssen – und das ist nicht ungefährlich. Eine Meta-Studie der Universitäten Greifswald und Bochum ergab, dass humane Coronaviren bis zu neun Tage auf Kunststoff- oder Metalloberflächen zumindest nachzuweisen sind. Verlässt man sich als Notlösung auf Endgeräte aus dem Consumer-Bereich, können diese schnell zum gefährlichen Virendepot werden – oder ganz ausfallen, denn auf häufige Desinfektion sind sie nun einmal nicht ausgelegt.

Patientenrufsystem aus dem „Notfallkoffer“

Dass es aber durchaus schnell ***und*** sicher geht, beweist ein Hilfskrankenhaus für 56 bis 90 Covid-19-Patienten, das binnen weniger Tage im Internat einer Hotelberufsschule eingerichtet wurde. Hier konnte das IT-Management auf einen vorkonfigurierten „Notfallkoffer“ auf der Basis des Ascom teleCARE IP Systems zurückgreifen. Dazu musste man nur die im Set enthaltenen mobilen Funk-Repeater an geeigneter Stelle platzieren und mit dem Stromnetz verbinden – fertig war das Patientenrufsystem. Die gesamte Installation nahm dabei weniger als eine Stunde in Anspruch. Jeder Patient erhält nun ein batteriebetriebenes Armband mit einem Alarmknopf. Sein Ruf wird direkt an ein Display im Koffer weitergeleitet und bleibt jederzeit nachverfolgbar. Weitgehend konform zur VDE-Richtlinie 0834, muss das System lediglich Kompromisse bei den Selbsttest-Intervallen eingehen, um eine einjährige Batterielebensdauer sicherzustellen.



Ascom d63 und Ascom Myco3: Die robusten Endgeräte eignen sich für sichere Funknetzwerke und lassen sich sogar mit der Medizintechnik verbinden. *Grafik: Ascom*



Beispiel eines Ad-hoc-Hilfskrankenhauses in einer umfunktionierten Sportstätte: Ein Funkkommunikationsnetz ist mit „DECT in a Box“ in kürzester Zeit aufgebaut. Grafik: Ascom

Kommunikation out of the Box

Ähnlich unkompliziert war ein Ad-hoc-Kommunikationssystem für die Pflegekräfte. Denn dafür gibt es mit „DECT in a Box“ ebenfalls eine Nachrüstlösung, basierend auf klinikerprobten Komponenten. Ein Server sowie mehrere per Kabel verbundene Basisstationen sorgen für eine zuverlässige DECT-Abdeckung. Als Endgeräte fungieren die bewährten Tastentelefone vom Typ Ascom d63. Die beiden Ad-hoc-Netze wurden anschließend miteinander verbunden, so dass alle Alarme zusätzlich auf den DECT-Telefonen angezeigt werden.

Grundsätzlich lassen sich Funkkommunikationssysteme sogar mit der Medizintechnik vernetzen, so dass zum Beispiel Alarme von Beatmungsgeräten nicht mehr nur akustisch gegeben werden, sondern direkt auf dem Endgerät der zuständigen Pflegekräfte erscheinen. Ein vordefiniertes Weiterleitungs- und Quittierungssystem garantiert dabei, dass kein Alarm übersehen oder doppelt verfolgt wird.

Desinfektionssichere Endgeräte

Alle diese Kommunikationssysteme können sich auf robuste Endgeräte stützen, die im Krankenhaus seit vielen Jahren sicher und erfolgreich im Einsatz sind. Dabei muss man keineswegs auf die Vorteile eines großflächigen und übersichtlichen Touchscreens verzichten. Spezielle Klinik-Smartphones wie das Ascom Myco3 vereinen die Funktionalität normaler Android-Consumer-Geräte mit Widerstandsfähigkeit gegen Stürze oder gängige Desinfektionsmittel. Die mehrmals tägliche Wischdesinfektion mit Ethanol oder Virkon S über längere Zeiträume kann den Endgeräten nichts anhaben.

Wie sich das Infektionsgeschehen in Deutschland weiter entwickeln wird, ist selbst für Fachleute nicht präzise vorherzusagen. Umso wichtiger ist es für das IT-Management, Notfallpläne für Expansion und Nutzungsänderungen bereitzuhalten. Moderne Funkkommunikation bietet hierfür praktikable und sichere Möglichkeiten. Ad-hoc-Netzwerke und gut zu desinfizierende Endgeräte spielen dabei eine entscheidende Rolle.

Erst recht bei einer zweiten Welle, denn bis dahin sollten wir vorbereitet sein.

Zum Autor:
Dr. Udo Jendrysiak ist Solution Market Manager Healthcare für Deutschland, Österreich & Schweiz bei der Ascom Deutschland GmbH

Konzept, Design und Funktionen unterstützen leichte Desinfektion und Patientenschutz

Monitore und Panel PC können zur Hygiene beitragen

Monitore und Panel PC, die in besonders kritischen Umgebungen wie Operationssälen und Intensivstationen eingesetzt werden, unterliegen strengen Sicherheitsanforderungen. Maßgeblich dabei ist die EN 60601, die für die elektromagnetische Sicherheit ganz klare Vorgaben macht. Dabei stehen verschiedene Fragen im Raum. Zum einen geht es darum, ob Anwender oder Patienten durch elektromagnetische Strahlung oder Fehlströme zu Schaden kommen können. Zum anderen muss sichergestellt sein, dass kein anderes Gerät im Raum durch abgestrahlte elektromagnetische Wellen in seiner Funktion beeinträchtigt oder gar beschädigt wird.

Eine verlässliche Kennzeichnung für hygieneoptimiertes Design ist die IP-Schutzklasse eines Gerätes. Sie bezeichnet den Schutz gegen Eindringen von Flüssigkeiten und Fremdkörpern, die zu einem Ausfall oder der Zerstörung der Elektronik führen können. Test und Zertifizierung muss dabei immer für das Gesamtsystem erfolgen und auf dem Typenschild ausgewiesen werden. Eine gängige Schutzklasse für Monitore und Panel PC ist IP 54: Die Geräte sind in einem hohen Maß gegen das Eindringen von Wasser und Staub geschützt. Das vereinfacht die Reinigung und Desinfektion, weil auch gefahrlos nass und nicht nur feucht gearbeitet werden darf.

Eine noch höhere Sicherheit gewährleistet die Deklaration und Registrierung als Medizinprodukt Klasse I nach dem Medizinproduktegesetz (MDD). Dort wird eine Vielzahl von erweiterten Risikobetrachtungen für die Dokumentation sowie die kontinuierliche Marktüberwachung nach der Inverkehrbringung gefordert. Die IT-Verantwortlichen und Systemintegratoren haben damit die Sicherheit, dass sie derart zertifizierte Monitore und Panel PC problemlos installieren können und eine erleichterte Systemzulassung erfolgen kann.

Sicher durch Design

Auch von Seiten des Designs und der Konstruktion können Hersteller ihre Kunden bei der Hygiene unterstützen. Ein vollflächiges Schutzglas, das mit dem Frontrahmen verklebt ist, gehört heute fast schon zum Standard. Es lässt sich schnell desinfizieren und hat den Vorteil gegenüber Kunststoff, dass es nicht verkratzt und brüchig wird – was Keimen ideale Rückzugsräume bieten würde. Zusätzlich können Glasfronten mit einem antibakteriellen Mittel auf Silberionen-Basis behandelt werden. Das wird aufgebracht, härtet aus, ist transparent und hält mehreren Desinfektionsgängen stand. Es unterdrückt den Keimbefall jedoch nur, es verhindert ihn nicht. Die Oberflächen der Geräte sollten mit antibakteriellen Lacken beschichtet sein. Auch dort können Silberionen eingearbeitet sein, die eine Vermehrung von Bakterienkulturen hemmen.

Wichtiger in der gesamten Hygienebetrachtung ist jedoch, dass das Gehäuse rundum geschlossen ist. Häufig finden sich jedoch Lüftungsschlitze am Gerät, in die Keime nicht nur eindringen, sondern durch die Verwendung von Kühllüftern aus dem Infektionsherd wieder ausgestoßen werden können. Ein Verzicht auf jedwede Lüftungsöffnungen und die Verwendung von Lüftern sollte bei der Geräteauswahl somit immer in Betracht gezogen werden.

Das Kühlkonzept ist für den Betrieb von Monitoren und Panel PC entscheidend. Je ausgefeilter, desto leistungsfähigere Prozessoren können eingesetzt werden. ADLINK entwickelt hierfür im eigenen Haus spezielle CPU-Boards, die eine direkte Prozessor-Anbindung an das Gehäuse ermöglichen. Das ausgefeilte Gehäusekonzept sorgt im Weiteren für optimierte Wärmeverteilung und -ableitung. Voraussetzung hierfür ist ein Aluminiumgehäuse. Das daraus resultierende Mehrgewicht und auch die etwas erhöhten Kosten gegenüber Kunststoffgehäusen werden durch die erzielten Positiveffekte bei weitem kompensiert. Zum einen wird die Wärmeverteilung wesentlich verbessert, was die Verwendung leistungsstarker Desktop-Prozessoren anstelle abgespeckter Mobilvarianten ermöglicht, ohne dass die Temperaturgrenzen der Gehäuseoberflächen in patientennahen Bereichen überschritten werden. Zum anderen sind diese Gehäuse wesentlich robuster gegen mechanische Beanspruchungen und länger haltbar. Kunststoff neigt dazu auszuhärten, wird dann brüchig und bekommt Haarrisse. Keimen werden so Rückzugsorte geliefert.

Die Zuverlässigkeit drahtloser Netzwerke, gerade in punkto Störanfälligkeit und Überlastung, ist nach wie vor nicht gegeben. Deshalb setzen viele Gesundheitseinrichtungen in kritischen Umgebungen auf die Integration von Monitoren und Panel PC in die vorhandene, drahtgebundene Infrastruktur. Router, Switches und Hubs sind in der Regel keine medizinzugelassenen Geräte. Da dort Medizintechnik mit Nicht-Medizintechnik im Rahmen einer elektrischen Verbindung zusammengefügt wird, sind Panel PC entsprechend mit galvanisch isolierten Schnittstellen ausgestattet.

Sicher durch Ergonomie

Auch eine intelligente Bedienoberfläche kann zur Hygiene beziehungsweise zur einfachen Desinfektion von Monitoren und Panel PC beitragen. Dabei haben sich Bedienkonzepte mit seitlichen Tasten oder solchen an der Rückseite als ergonomisch suboptimal erwiesen, speziell bei größeren Bilddiagonalen. Darum sollten Touchscreens, die sich auch mit Hygienehandschuhen bedienen lassen, mittlerweile Standard sein. Auf Eingabegeräte wie Tastaturen und Mäuse kann man dann verzichten. Auch sogenannte kapazitive Touch-Tasten, die in der Glasoberfläche auch die Bedienung des PCs selbst ermöglichen, sind zu empfehlen. Damit ist die komplette Bedienung frontseitig hinter Glas sichergestellt, auch mit einer Abschaltfunktion des Touchscreens zum Reinigen und Desinfizieren der Oberfläche.

Die Funktionalitäten sollten nicht nur an der Vorderseite wählbar, sondern auch intuitiv bedienbar sein – mit so wenigen Tasten wie möglich und ohne tiefe Menüs. Nice-to-have sind darüber hinaus spezielle Tasten, deren Belegung jeder Anwender individuell konfigurieren kann.

André Fortdran
Product Marketing Manager Medical
ADLINK Technology GmbH
E-Mail: andre.fortdran@adlinktech.com
Telefon: 09 91 / 29 09 4 21 4

Patienten sollen Datenhoheit und Eigenverantwortung übernehmen

Interoperabilität für Patientendaten: in USA nun ein Muss

Geplant war die offizielle Bekanntgabe auf der HIMSS 2020; das Corona-Virus machte den Veranstaltern einen Strich durch die Rechnung. Und so kam die folgenreiche Ansage nicht aus Florida, sondern direkt aus Washington D.C.: Neue US-Regularien fordern den uneingeschränkten Zugriff auf Patientendaten – dank Interoperabilität. Eine API, ein Programmierinterface, macht die Forderung unausweichlich konkret.

Patienten sind abhängig von der Verfügbarkeit ihrer Daten innerhalb ihrer Behandlungskette, unterstreicht Lynda Rowe die Bedeutung der neuen Vorgaben. Sie arbeitet als Senior Advisor for Value-Based Markets bei InterSystems. Bereits seit zwei Jahrzehnten hat sie verantwortliche Positionen in der US-Gesundheits-IT inne; Interoperabilität spielt für ihr Engagement seit langem eine wichtige Rolle. So war sie an der Vorbereitung und am Aufbau von Health Information Exchanges (Datendrehscheiben) in den Bundesstaaten Massachusetts und New York sowie am Meaningful-Use-Programm der Regierungseinrichtung ONC beteiligt. Das Ziel: durch Verfügbarkeit relevanter Daten die Patientenversorgung verbessern.

Das Gesetzespaket regelt den uneingeschränkten Zugriff der Patienten auf ihre Daten bei öffentlichen und privaten Gesundheitsanbietern. Somit, so Dr. Stephan Schug, geht es weit über die US-Datenzugriffsinitiative Medicare Blue Button 2.0 hinaus, die nur öffentliche Leistungserbringer einbezog. Der Zugriff ist deutlich konkreter gefasst als beim deutschen Patientendatenschutzgesetz (PDSG), vergleicht der Chief Medical Officer und Partner im Management Team der European Health Telematics Association (EHTEL).

In die Pflicht nehmen die Vorgaben die IT-Anbieter ebenso wie Leistungserbringer und Kostenträger: Jeder US-Bürger soll – ohne besonderen Aufwand und ohne besondere technische Mittel – sämtliche elektronischen Daten einsehen, zur Verfügung gestellt bekommen und nutzen können, die für seine Gesundheit von Bedeutung sind – so das zentrale Ziel der beiden neuen „bahnbrechenden" Regelungen. Sie kommen aus dem Office of the National Coordinator for Health Information Technology (ONC) im U.S. Department of Health and Human Services (HHS), also dem Gesundheitsministerium, und von den Centers for Medicare & Medicaid Services (CMS). Die Regeln setzen Bestimmungen um, die der 21st Century Cures Act (Cures Act) vorgegeben hatte, und untermauern die MyHealthEData.Initiative von Präsident Trump.

Die Regeln sollen die US-Amerikaner zur Übernahme von Verantwortung für die eigene Gesundheit befähigen und so den Patientennutzen in den Mittelpunkt der Versorgung rücken. Der Zwang, ab 2021 den Zugriff auf Patientendaten zu ermöglichen, das Vorantreiben von Innovation etwa durch Smartphone-Apps und das Aus von Brüchen im Informationsfluss dienen diesen Zielen.

Die API ersetzt „zahnlose" Empfehlungen

Standards für Interoperabilität sind eher Rahmen mit Freiräumen, betont Rowe. Schnittstellenprobleme sind durch sie „vorprogrammiert". Das Gesetzespaket macht nun Schluss mit schwer zu findenden „Seiteneingängen": Alle Gesundheitsanbieter, bzw. ihre Lösungshersteller, müssen eine universelle, mit dem Standard-Release FHIR 4 kompatible „Patienten-API" realisieren. Dies ermöglicht den weitgehend ungehinderten Zugriff auf die Daten durch Apps, urteilt Dr. Schug. Ein großer US-KIS-Anbieter versuchte daher, die Verabschiedung des Gesetzespakets zu verhindern. Andererseits unterstützten Apple, Google und Co. die neuen Regeln vehement, da sie ja mit ihren Apps und Services vom ungehinderten Datenzugriff profitieren.

Die Patienten sind abhängig von der Verfügbarkeit ihrer Daten innerhalb ihrer Behandlungskette: Lynda Rowe, Senior Advisor for Value-Based Markets, InterSystems

Der Zugriff durch Patienten laut US-Gesetzespaket ist deutlich konkreter gefasst als beim deutschen Patientendatenschutzgesetz (PDSG): Dr. Stephan Schug, Chief Medical Officer und Partner im Management Team der European Health Telematics Association (EHTEL)

Während hierzulande laut PDSG der Patient auf die einmal befüllte Patientenakte mit seinem Smartphone zugreifen kann, müssen Daten erst einmal durch persönliche Intervention von Seiten der Leistungserbringer in die EPA eingespeist werden. In den USA lassen sich hingegen Daten künftig per API aus jedem System auslesen. Dabei lässt die ONC-Regelung Gebühren in „angemessener Form" zu. Um den Zugriff zu ermöglichen, müssen die Provider sich in ein Online-Verzeichnis eintragen und die dezentralen Schnittstellen „rund um die Uhr" betreiben. – In Europa, so Dr. Schug empfahlen eHealth-Aktionspläne nur einen weitgehend zentralisierten online-Zugriff von Patienten auf ihre Gesundheitsdaten, und dies jeweils im nationalen Kontext.

Schluss mit „Information Blocking"

Das Blockieren der Weitergabe von Patientendaten ist in den USA künftig strafbewehrt, wenn auch durch COVID-19 verzögert mit Wirkung frühestens in einigen Monaten. Dr. Schug vergleicht dies mit den Sanktionen für die Nichtanbindung von Niedergelassenen, Psychotherapeuten etc. sowie von Krankenhäusern und Apotheken an die Telematikinfrastruktur durch spürbare Abzüge bei der Vergütung. Die ONC-Anforderungen gelten für Leistungserbringer ebenso wie für Anbieter zertifizierter Lösungen, Netzwerke bzw. Plattformen. Sie umfassen den Austausch von Gesundheitsinformationen – Daten, Texte, Bilder und Kontextinformationen. Als Sanktion setzt man in den USA auch auf die Veröffentlichung einer Liste der Interoperabilitäts-Verweigerer; deren Wirksamkeit hinterfragt allerdings Rowe.

Auf die Vereinbarung eines Minimaldatensatzes, der in der ersten Stufe Anforderungen an die Kodierung „in mittlerer Strenge" stellt, lenkt Dr. Schug ebenfalls die Aufmerksamkeit. Der Vorgabenkatalog USCDI (U.S. Core Data for Interoperability) schreibt für jedes Daten-Item verbindlich eine Kodierung fest, etwa LOINC für Labordaten, UCUM-Maßeinheiten, RxNorm – das amerikanische Nomenklatur- und Kodiersystem für Medizinalprodukte und an zahlreichen Stellen SNOMED CT. Der Experte zieht hier den Vergleich zu Deutschland mit dem Notfalldatensatz und den ersten Implementierungen des International Patient Summary (IPS). Ähnlichkeiten bei der Art der Festlegung sieht er ferner bei den Medizinischen Informationsobjekten (MIOs) und – viel breiter aufgestellt als in den USA – beim Kerndatensatz der Medizininformatik-Initiative.

Die EU-Empfehlungen für ein europäisches Austauschdatenformat zu elektronischen Patientenakten (EHRxF) sehen unter Bezug auf IPS, HL7 CDA und FHIR etc. eine stufenweise Herstellung von Interoperabilität vor, so Dr. Schug weiter.

Mit der strafbewehrten, medienbruchfreien Verfügbarkeit der Basisdaten sind die USA der EU und Deutschland nun einen Schritt voraus, so das Urteil des EHTEL-Vertreters. Die Betonung der medizinischen Gesamtprozesse, etwa die Ausrichtung der Basisdokumentation zur Verwendung beim Disease Management, findet er bei den Amerikanern ebenso positiv.

Die ONC-Regelung gibt vor, dass elektronische Patientenakten die klinischen Daten inklusive der Kerndatenklassen und -elemente verfügbar machen müssen, um neue Geschäftsmodelle für die Leistungserbringung zu ermöglichen. Dies hat auf Basis des USCDI-Standardsets an Klassen für Gesundheitsdaten und Datenelementen zu geschehen, die für einen nationalen interoperablen Datenaustausch notwendig sind – etwa klinische Notizen und Angaben zu Allergien sowie zur Medikamentierung oder essenzielle demographische Informationen.

Große Potenziale für App-Anbieter und Kostenträger dank API

Das ONC hat in seiner Regelung die Spezifikationen für eine sichere, Standard-basierte API festgelegt. Sie sollen den Zugriff der Patienten und die Souveränität über die Daten des jeweiligen Leistungserbringers sicherstellen – kostenfrei per Smartphone. Dr. Schug kommentiert, US-Patienten öffentlicher Gesundheitsanbieter hätten ja mit Blue Button 2.0 bereits umfangreichen Zugriff auf ihre Gesundheits- und auch ihre Abrechnungsdaten. Drumherum hat sich bereits ein umfangreicher Marktplatz für innovative Apps entwickelt. Die neue Regelung weitet das offenbar massiv aus. Das Unter-Strafe-Stellen von Information Blocking bedeute auch, dass die Daten in verständlicher Form verfügbar zu machen sind.

Ähnliches, so der EHTEL-Manager, praktizieren die deutschen Krankenkassen, etwa die TK mit ihren EPA-Apps, bereits seit einiger Zeit, allerdings nur in der jeweils hauseigenen App – nicht mit Verfügbarkeit über eine API universell für Entwickler und Services. Seitens der EU habe sich in diesem Kontext zwar ein Code of Conduct für App-Anbieter entwickelt, für die Nutzung medizinischer Daten seien die Anstrengungen jedoch ohne Ergebnis geblieben.

Die CMS-Regelung zu Interoperabilität und Zugriff für Patienten gibt den Stakeholdern mit Leistungsangeboten für

Schluss mit den verteilten Verantwortlichkeiten in Deutschland: Alexander Ihls, Gründungsvorsitzender IHE-D, Member At-Large IHE International Board, sowie Vorstandsmitglied AK eHealth des Bitkom und im Vorstand des Spitzenverbandes IT-Standards im Gesundheitswesen (SiTIG), auf einer DMEA

Medicare Advantage, Medicaid und CHIP und allgemein Leistungserbringern mit US-weitem Aktionsradius vor, Abrechnungsdaten elektronisch Patienten zur Verfügung zu stellen. Medicare hatte 2018 hierzu mit Blue Button 2.0 den Grundstein gelegt – und es Entwicklern ermöglicht, Medicare-Patienten innovative Lösungen anzubieten. Ab 1. Januar 2021 müssen die Leistungs-Stakeholder Gesundheitsdaten sicher und in verständlicher Form über die API mit Patienten austauschen. Wer also weiter als Leistungserbringer für Medicare und Medicaid agieren möchte, muss elektronisch Informationen über Aufnahme, Entlassung über Überweisung von Patienten an Partner in der Behandlungskette verschicken.

Kostenträger müssen laut den neuen Vorgaben neben Patientendaten auch Übersichten zu den Leistungserbringern verfügbar machen, die bei ihnen unter Vertrag stehen. Interoperabilitätsspezialisten wie InterSystems bieten auch hier Unterstützung – etwa durch HealthShare und die Integrations- und Entwicklungsplattform Iris for Health, mit denen sich die Daten für die geforderte API unter Berücksichtigung der Datentypen von USCDI umsetzen lassen.

Nutzeffekt dank Konkretisierung

Was lernen wir hieraus für die Gesundheits-IT in Deutschland? „Machen wir Schluss mit den verteilten Verantwortlichkeiten in Deutschland", fordert der Interoperabilitätsexperte Alexander Ihls. „Die neuen Regelungen, insbesondere die API-Spezifizierungen, definieren für alle amerikanischen Leistungserbringer, Kostenträger und Lösungsanbieter einheitliche Grundlagen für IT-Nutzenpotenziale für den Patienten und für das Gesamtsystem. So könnten wir auch hierzulande besser vorankommen!", so Ihls, Gründungsvorsitzender IHE-D, Member At-Large IHE International Board, sowie Vorstandsmitglied AK eHealth des Bitkom und im Vorstand des Spitzenverbandes IT-Standards im Gesundheitswesen (SiTIG).

Manche Patienten, denkt Rowe, werden nicht selbst auf ihre Daten zugreifen wollen. Aber von ihrem Leistungserbringer werden sie dies erwarten. Andere werden souverän mit ihren Daten umgehen wollen. Die Expertin erinnert an den alten Streit – gehören Patientendaten den Patienten oder den Leistungserbringern? Ärzte sind nur „Stewards" der Information, unterstreicht Rowe. Auch wenn dies nur punktuell gewünscht sein mag – die Daten müssen dem Patienten zur Verfügung stehen und seiner Steuerung unterliegen. Dabei gilt: „Schluss mit überhöhten Gebühren für Kopien. Weg mit Fax!".

„Wie sieht nun mein Ökosystem aus?": Die neuen Regeln werden ein Signal an Anbieter und Leistungserbringer sein, sich neu zu erfinden, so Rowes Erwartung. Leistungserbringer und Patienten bzw. Patientenvertreter können profitieren. Ihre Aufforderung an IT- und Medizintechnikanbieter lautet: „Seid Partner, statt Silos zu bilden!". Die Systeme bleiben zwar weiter proprietär, aber entstehende Daten müssen ausnahmslos interoperabel sein. Dies gilt für medizinische Daten ebenso wie etwa für gesundheitsrelevante Sozialdaten. Und auch Rowe weist hierauf hin: Einsteigern von außen wird die Teilnahme am Markt erleichtert – etwa Google, Apple und Amazon.

Autor: Michael Reiter

Interoperabilität ermöglicht den gesamtheitlichen Blick auf Patienten: Don Woodlock, Vice President, InterSystems HealthShare, auf einem Jahreskongress der HIMSS

Sicherer, leichter Austausch von Daten über Hubs

Gute Versorgung bedeutet: Behandler müssen einen gesamtheitlichen Blick auf ihre Patienten erhalten, die mitunter viele verschiedene Ärzte sehen, unterstreicht Don Woodlock, Vice President, InterSystems HealthShare. Mit diesem Ziel ermöglichen landesweit föderierte Netzwerke wie CommonWell Health Alliance und Carequality den an der Versorgung Beteiligten einen sicheren, bequemen Austausch von Patientendaten. Die HealthShare-Plattform von InterSystems schafft die Grundlagen und Werkzeuge dafür, dass über diese Stakeholder hinweg Daten zugreifbar werden – unabhängig von eingesetzten Applikationen wie etwa KIS-Lösungen.

„Dank solcher ‚Marktplätze' können Patienten sicher sein, dass ihrem Arzt alle Daten zu ihrer Erkrankung zur Verfügung stehen – und er sie somit besser behandeln kann", betont Woodlock. Interoperabilität stellt Akteure bislang vor komplexe Anforderungen; die neuen Regeln aus Washington reduzieren mit ihrer Konkretisierung von Details diese Komplexität, sagt Woodlock. Das macht es nun leichter, neue Ökosysteme aus partnerschaftlichen Akteuren aufzubauen.

Wie sichere mobile Technologien die Patientenversorgung verbessern können

von Stefan Mennecke, Vice President of Sales Eastern and Central Europe bei SOTI

Im Zuge des technologischen Fortschritts greift das Gesundheitssystem in Deutschland immer stärker auf mobile Geräte zurück, um wichtige Aufgaben bei der Patientenbetreuung zu erfüllen. Der technologische Fortschritt betrifft sowohl medizinische Geräte als auch Geräte, die bei der Erfassung und Aktualisierung von Patientendaten eingesetzt werden, beispielsweise in der Pflege und der Forschung. Gesundheitsminister Jens Spahn möchte ab 2021 sogar eine digitale Patientenakte [1] einführen, die medizinischem Personal die relevanten Patientendaten gebündelt bereitstellt.

Die rasche Zunahme mobiler Technologien im Gesundheitswesen und die Verbreitung des Internets der Dinge (IoT) in Unternehmen hat aber auch zahlreiche Risiken und Herausforderungen mit sich gebracht. In der modernen Welt des IoT werden im Gesundheitswesen Milliarden neuer Geräte im Einsatz sein, die eine Vielzahl von Funktionen, Verbindungen, Standards und Protokollen enthalten. Einige der häufig verwendeten Geräte sind relativ simpel aufgebaut, wie berührungslose oder intelligente Thermometer, und Sicherheitsrisiken sind der Sache nach gering. Jedoch in Hinblick auf andere Geräte, die sensible Patientendaten enthalten, müssen die Anbieter unbedingt Schritte unternehmen, um die notwendigen Sicherheitsprotokolle und -systeme im Einsatz zu haben.

Man stelle sich 100 dieser Thermometer in einem durchschnittlichen Krankenhaus vor, die alle an das Netzwerk angeschlossen sind, um die Temperaturmesswerte an eine zentrale Datenbank zu übermitteln. Wenn diese Geräte unsachgemäß verwaltet und somit unsicher sind, bleiben 100 offene Endpunkte, die bei einem Cyberangriff ausgenutzt werden könnten.

Nur technisch versierte Gesundheitsdienstleister sind in der Lage, hochwertigen Service zu bieten

In komplexen medizinischen Umgebungen werden an Arbeitnehmer eine ganze Reihe von zeitaufwendigen Vorschriften gestellt. Von der Aufnahme von Patienten bis hin zur Verwaltung von Medikamenten und Krankenakten gibt es viele Verwaltungsaufgaben, die eine effektive Arbeit und ein hohes Maß an Betreuung unmöglich machen.

Wie in vielen anderen Branchen hat die Mobilität moderner Endgeräte einen großen Einfluss auf das Gesundheitswesen und die häusliche Pflege. Ärzte, Krankenschwestern und Pflegepersonal werden zunehmend mobile Endgeräte nutzen und tagtäglich für klinische und nicht-klinische Aktivitäten wie Verwaltungsaufgaben einsetzen. Patientenmonitore, Infusionspumpen oder diagnostische Bildgebungslösungen werden zunehmend mobil – ein großer Fortschritt für die Diagnostik und die Behandlung von Patienten. Relevante Daten sind zu jeder Zeit abrufbar, Prozesse werden beschleunigt und individuelle therapeutische Anpassungsvorgänge verkürzt. Ein Mehrwert, nicht nur für klinische Abteilungen, sondern auch im Bereich der Pflege und der wachsenden Verwaltungsaufgaben. Dies ermöglicht eine völlig neue Qualität an Flexibilität und Prozessgeschwindigkeit.

Die Einführung mobiler Technologien in die Prozesse des Gesundheitswesens hat also zahlreiche Vorteile. Die Ausstattung des Personals mit der neuesten Mobiltechnologie ermöglicht es den Mitarbeitern, auf einfache und präzise Weise zu überwachen, zu dokumentieren und zu kommunizieren, um eine sorgfältige und effizientere Versorgung der Patienten zu erreichen.

Nach Angaben von Honeywell, einem weltweiten Anbieter von Technologielösungen, sind über 38% der Anbieter im Gesundheitswesen der Ansicht, dass ein schneller und bequemer Service für die Patienten höchste Priorität hat. Ärzte selbst verbringen jedoch durchschnittlich 43% ihrer Zeit mit der Dokumentation und nur 28% ihrer Zeit mit dem direkten Kontakt zum Patienten [2]. Mit einer erfolgreichen Einführung digitaler Technologien werden Gesundheitseinrichtungen ihren Patienten einen qualitativ hochwertigen Service bei höherer Präzisionsrate können.

Daten im Gesundheitswesen sind gefährdet

Bis zum Jahr 2020 wird der digitale Gesundheitsmarkt auf über 200 Milliarden US-Dollar [3] anwachsen. Im Zuge dessen werden immer mehr hochtechnisierte, computerbasierte medizinische und systemsteuernde Geräte mit entsprechend installierten Betriebssystemen und Anwendungen in modernen Kliniken und Gesundheitseinrichtungen zum Einsatz kommen. Demzufolge wird die Menge anfallender Daten stark anwachsen. Während die Einführung mobiler Technologien, die

NEXUS / DeepView

DURCHBLICK IN DER TIEFE

Wir könnten es HCM, ECM, VNA, Repository oder PACS+ nennen. Tun wir aber nicht ... denn NEXUS / DeepView ist MEHR!

nexus|ag
www.nexus-ag.de

es den Mitarbeitern ermöglichen effizienter zu arbeiten und Patienten besser zu versorgen, im Gesundheitssektor viele Vorteile mit sich bringt, birgt zugleich die wachsende Zahl von Geräten, die private Patientendaten verarbeiten, auch Risiken für die Datensicherheit. Seien es Informationen zu Krankheiten, der medizinischen Vorgeschichte oder dem Umfang aktueller Medikationspläne von Patienten – solch äußerst private Informationen dürften wohl zu den kritischsten zählen.

Im Juli 2019 mussten sich einige Krankenhäuser in Rheinland-Pfalz und im Saarland gegen einen Hackerangriff zur Wehr setzen. Das komplette Netzwerk des DRK Verbands Süd-West war betroffen. Die Gesundheitsministerin von Rheinland-Pfalz forderte daraufhin mehr Budget auch für kleinere Krankenhäuser, um in die IT-Sicherheit investieren zu können. Die Zunahme von Cyberangriffen, die sich gegen den Gesundheitssektor richten, gefährdet sowohl die Gesundheit als auch die privaten Informationen vieler Deutscher. Eine Studie von Roland Berger [4] fand heraus, dass 2017 bereits 64 Prozent aller Kliniken in Deutschland Opfer eines Cyberangriffs waren. Eine kürzlich durchgeführte Umfrage von SOTI, Racing Towards the Future of Enterprise Mobility [5], ergab, dass heute nur 35 % der IT-Administratoren im Gesundheitswesen mit Bildgebungs-, Medizin- oder Wissenschaftstechnologie zu tun haben. Es ist jedoch bekannt, dass mobile Technologie in jedem Bereich der Industrie zu finden ist. Somit ist es unerlässlich, dass eine gut vernetzte geschäftskritische Mobilitätsstrategie im Einsatz ist, bevor die Geräte in einem Gesundheitsökosystem eingesetzt werden.

Führende Unternehmen der Gesundheitsbranche müssen erkennen, dass die Bereitstellung von Echtzeit-Dienstleistungen ebenfalls die Ausstattung ihrer Mitarbeiter mit vernetzten, mobilen Technologien umfasst, die es ihnen ermöglichen, den Patienten eine gleichbleibend hohe Versorgungsqualität zu bieten. Dazu gehört auch, dass den Mitarbeitern vor Ort die entsprechende Unterstützung zur Verfügung gestellt wird, wenn sie Probleme mit ihren mobilen Geräten haben.

Eine geschäftskritische Mobilitätslösung, die alle digitalen Plattformen und Geräte im Gesundheitswesen integriert, stellt sicher, dass das gesamte System zuverlässig und sicher läuft. Dank der Möglichkeiten der Fernverwaltung lassen sich abhandengekommene oder kompromittierte Geräte aus der Ferne sperren und Benutzer-Freigaben mit unterschiedlichen Sicherheitsebenen erstellen. Dies bedeutet, dass ein Gerät von verschiedenen Mitarbeitern verwendet werden kann und jeweils Zugang zu der spezifischen Informationsebene gewährleistet ist, ohne unnötige Sicherheitsrisiken einzugehen.

Weitere wichtige Schutzmechanismen sind das sogenannte Geo-Fencing und ein integrierter Lockdown-Modus. Dabei handelt es sich um eine Technologie, bei der Daten lediglich in einem ausgewählten lokalen Bereich abrufbar sind – etwa innerhalb eines Krankenhauses. Verlässt ein Endgerät dieses klar umrissene Areal, wird der Zugriff auf die geschützten Informationen automatisch verweigert. Durch den Lockdown-Modus können auf allen Geräten nur im Vorfeld genehmigte Applikationen verwendet und Einstellungen lediglich vom IT-Team vorgenommen werden können. Auf diese Weise kann ein potenzieller Missbrauch von Daten durch schädliche Apps verhindert und die Weitergabe sensibler Informationen an organisationsfremde Applikationen unterbunden werden. Um all diese Funktionalitäten unkompliziert und zentral steuern zu können, kann ein IT-Team im Fernwartungsmodus standortunabhängig auf alle Geräte zugreifen und etwaig auftretende Probleme beheben. Außerdem können so sicherheitsrelevante Updates für ein Gerät sowie die darauf verwendeten Apps eingespielt und so Sicherheitslücken einfach und schnell geschlossen werden.

Integration von Mobiltechnologie ebnet den Weg für moderne Gesundheitsdienste

Die Implementierung von Mobilität führt zu effizienteren Arbeitsabläufen und verbessert die Patientenversorgung im deutschen Gesundheitswesen. Die wachsende Zahl der dort eingesetzten mobilen Geräte beinhaltet jedoch Risiken. Da die Anbieter im Gesundheitswesen verstärkt auf digitale Systeme und ihre Daten zurückgreifen, um die Qualität der Gesundheitsversorgung zu erhöhen, müssen sie die Sicherheit und Verfügbarkeit dieser Informationen stets durch geeignetes sicheres Mobilitäts- und IoT-Management gewährleisten.

Quellen:

[1] https://www.deutschlandfunk.de/gesundheitswesen-digitale-patientenakte-ab-2021.740.de.html?dram:article_id=452546

[2] Honeywell eBook: Welcome to the patient care revolution (2019)

[3] https://www.rolandberger.com/de/Media/Digitaler-Gesundheitsmarkt-wächst-bis-2020-um-durchschnittlich-21-Prozent-pro-Ja.html

[4] https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2017.pdf

[5] https://contest.soti.net/media/2331/soti-future-of-enterprise-mobility-report.pdf

IT Sicherheit im Krankenhaus

Journal für Strategie und Praxis

9. KRITIScher Stammtisch zum IT-Sicherheitsgesetz Sektor Gesundheit

Corona und die KRITIS-Audits

Der KRITIScher Stammtisch wird seit 2017 auf Initiative des Universitätsklinikums Carl Gustav Carus Dresden zusammen mit der SHD System-Haus-Dresden GmbH durchgeführt. Neben der Wissensvermittlung durch KRITIS-Experten steht vor allem der Erfahrungs- und Meinungsaustausch mit den Teilnehmern im Vordergrund. Die Veranstaltung hat sich als erfolgreiches Konzept weit über die mitteldeutschen Landesgrenzen hinaus etabliert und bietet Vertretern von Krankenhäusern die Möglichkeit des exklusiven Erfahrungsaustausches.

Das IT-Sicherheitsgesetz des Bundes und die KRITIS-Verordnung haben den Schutz „kritischer Infrastrukturen" zur Aufrechterhaltung wichtiger gesellschaftlicher Funktionen im Fokus. Im Gesundheitswesen betrifft es Krankenhäuser mit über 30.000 stationären Fällen pro Jahr. Aber auch kleineren Häusern wird angeraten, sich an den Branchenstandard B3S zu halten.

Aufgrund der Corona-Pandemie wurde der 9. KRITIScher Stammtisch als virtuelle Veranstaltung am 14. Mai 2020 durchgeführt. Rund 40 Teilnehmer trafen sich über ein Meeting-Tool, um über das IT-Sicherheitsgesetz zu diskutieren und Erfahrungen auszutauschen.

Mehr Angriffe, aber weniger Anzeigen

Mike Zimmermann, IT-Sicherheitsbeauftragter am Universitätsklinikum Carl Gustav Carus Dresden gab Einblicke in die aktuelle Lage aus dem UP KRITIS Branchenarbeitskreis (BAK) Medizinische Versorgung. Die gegenwärtige Corona-Pandemie bedeute für die IT enorme Herausforderungen, da man in kürzester Zeit neue bzw. geänderte Anforderungen bei Themen wie zu, Beispiel Home Office, Konferenz/Kollaboration Tools, Beschaffung mobiler IT-Systeme umsetzen müsse, betonte Zimmermann.

Zudem gab er zu bedenken, dass es zugleich ein Surfbrett für Angreifer sei und die IT-Sicherheit vor große Herausforderung stelle. Insgesamt gibt es zwar mehr Angriffe auf die IT,

doch Eric Fischer, Zentrale Ansprechstelle Cybercrime (ZAC), Landeskriminalamt Sachsen, erklärte in seinem Vortrag, dass es kaum mehr Anzeigen gäbe. „Das Anzeige-Verhalten ist extrem eingebrochen. Vielleicht haben die Leute momentan andere Probleme.", gab Fischer zu bedenken. Es gebe ein sehr hohes Dunkelfeld bezüglich der Angriffe auf die IT-Sicherheit.

René Salamon, Sektorbetreuer Gesundheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI), erklärte, dass die Angriffe durch eine gute Sensibilisierung der Mitarbeiter für die IT-Sicherheit gut abgewehrt werden könnten. Diese Rückmeldung habe er aus den Krankenhäusern erhalten, so Salamon. So habe die Corona-Krise dazu geführt, dass die Abteilungen mehr zusammengewachsen seien, die Regeln der IT würden besser eingehalten und diese Ruhe könne genutzt werden, um sich für die gravierenden Fälle zu wappnen.

Fristverschiebung durch Corona?

Auch wenn Corona die gegenwärtige Lage durcheinanderbringt, so müssen die Fristen zur Erfüllung der Vorgaben eingehalten werden. René Salamon, Sektorbetreuer Gesundheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI), appellierte an alle Krankenhäuser, sich rechtzeitig um eine Prüfstelle zu kümmern. Markus Holzbrecher-Morys, Deutsche Krankenhausgesellschaft e. V., Geschäftsführer Datenaustausch, IT-Sicherheit und Digitalisierung, betonte, dass die DKG sich täglich intensiv mit der Corona-Gesetzgebung beschäftige. Das Problem sei aber, so Holzbrecher-Morys, dass die verschiedenen Gesetzes- und Verordnungsentwürfe mit äußerst kurzen Vorlauffristen auf die Krankenhäuser zukämen und teils nicht immer eindeutig seien. So träten immer wieder versteckte Abhängigkeiten auf, die „nicht auf dem Schirm waren." Die Menge der nun gesetzlich umzusetzenden IT-Themen, angefangen bei neuen Informationspflichten bis hin zum Aufbau neuer Corona-Behandlungszentren, würden die Informationstechnik und die dafür zuständigen Mitarbeiterinnen und Mitarbeiter in den Kliniken insgesamt vor große Herausforderungen stellen. Trotzdem dürfe die IT-Sicherheit gerade jetzt nicht aus dem Blick geraten.

Zudem erklärte Holzbrecher-Morys, dass die DKG eine Umfrage an KRITIS-Häuser verschickt habe, um Rückmeldungen zum Audit-Verfahren aus 2019 zu erhalten, die auch bei der weiteren Überarbeitung de B3S berücksichtigt werden sollen. Eine bislang positive Rückmeldequote lasse auf aussagekräftige Ergebnisse hoffen, so Holzbrecher-Morys. Die Ergebnisse würden im Herbst diesen Jahres in anonymisierter Form der Öffentlichkeit zugänglich gemacht. Ein transparenter Umgang mit den Themen sei auch eine Hilfe für andere Häuser.

Erfahrungsbericht Software-Plattform (aeneis)

Mike Zimmermann, IT-Sicherheitsbeauftragter des Universitätsklinikums Carl Gustav Carus, Philipp Klanert und Jens Höhnel, beide SHD, stellten in ihrem Vortrag das webbasierte Tool ISMS@aeneis mit integrierten B3S Krankenhaus/ISO27001 sowie des DSGVO@aeneis auf Basis der Software-Plattform (aeneis) vor und berichteten über ihre direkten Erfahrungen.

Handlungsempfehlung zum Einsatz Konferenz-Tools im Krankenhaus

Viele Krankenhäuser haben nicht die Ressourcen, aus dem „BSI Kompendium Videokonferenzsysteme KoViKo - Version 1.0.1" eine für die Praxis handhabbare Handlungsanweisung zu erstellen.

Aus diesem Grunde wurde für den Teilnehmerkreis des KRITISchen Stammtisches von Mike Zimmerman und Konrad Christoph die „Handlungsempfehlung Konferenz-Tools Version 0.4" erarbeitet. Diese soll eine erste Diskussionsgrundlage sein, die Empfehlungen aus dem BSI KoViKo in die Krankenhaus-Praxis umzusetzen. Spontan wurde im Verlaufe des virtuellen KRITISchen Stammtisches die Idee einer Arbeitsgruppe geboren, um die Handlungsempfehlung weiter zu entwickeln. Interessenten sind herzlich zur Mitarbeit eingeladen.

10. KRITIScher Stammtisch

Der Organisator, Konrad Christoph, Teamleiter Gesundheitswesen, SHD, wies zum Abschluss auf den nächsten Stammtisch hin, der für den 10. September 2020 geplant sei. Zudem feiert die SHD das 30jährige Firmenjubiläum. In welcher Form der nächste Stammtisch stattfinden wird, virtuell oder als reales Treffen, wird dann entsprechend der dann herrschenden Lage entschieden. ***df***

„Wo vertrauliche Daten wie im Gesundheitswesen betroffen sind, sind Cyberkriminelle nicht weit“

Die aktuelle Situation zeigt, wie wichtig eine effiziente Digitalisierung ist. Doch auch die Auswirkungen auf die IT-Sicherheit stellen die Akteure verstärkt vor große und neue Herausforderungen.

Das ist beides richtig. Einerseits beleuchten die aktuellen Ereignisse die Wichtigkeit kritischer Infrastrukturen, die nun schon seit Wochen stark beansprucht werden. Wenn in einer solchen Ausnahmesituation wie der Corona-Pandemie etwas so Exponiertes wie IT-Umgebungen im Gesundheitswesen ausfallen würden, wäre das längst nicht nur ein technisches Problem – im schlimmsten Falle wären es Menschenleben, die auf dem Spiel stünden.

Andererseits zeigt sich die ganze Widersprüchlichkeit der Situation: Man sieht die harte Arbeit, die beispielsweise Ärzte und Pflegekräfte tagtäglich leisten, man spürt den menschlichen Zusammenhalt in der Gesellschaft – und gleichzeitig werden die wirtschaftlichen Interessen deutlich. Ich denke da an Atemschutzmasken, bei denen es zuerst einen sprunghaften Preisanstieg und dann millionenschwere Betrugsfälle zu verzeichnen gab. Ganz zu schweigen von den Geldern, um die es bei der alles überlagernden Impfstoffsuche geht.

Und wo wirtschaftliche Interessen, vertrauliche Daten oder hochsensible IT-Systeme – wie eben im Gesundheitswesen – betroffen sind, sind Cyberkriminelle nie weit.

Welche Innovationen können Sie im Krisenjahr 2020 präsentieren? Welche Themen möchten Sie in den Vordergrund rücken?

Auch bei uns stand das Jahr 2018 ganz im Zeichen der Europäischen Datenschutz-Grundverordnung. 2019 konnten wir dann einen echten Meilenstein vorstellen: Die QUICK-Technology, mit der wir der verschlüsselten E-Mail-Kommunikation zum flächendeckenden Durchbruch verhelfen möchten. Sie beseitigt die Komplexität bei der Verschlüsselung von Dateien und E-Mails – und beschleunigt so die Kommunikationsvorgänge zwischen regelmäßig miteinander korrespondierenden Anwendern deutlich.

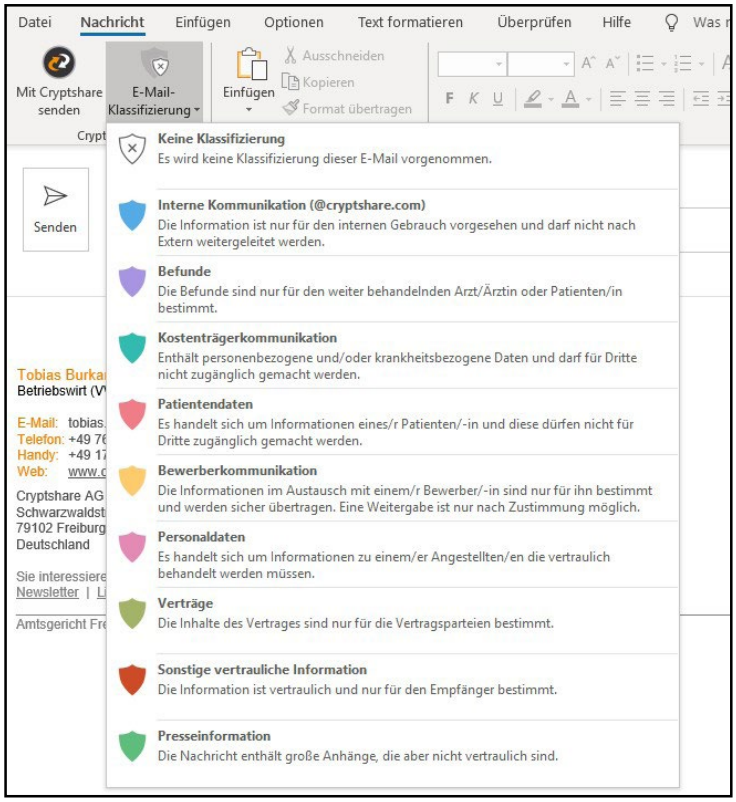
Darauf bauen wir nun auf. Neben der Weiterentwicklung von QUICK steht 2020 der Ausbau unseres Engagements in der Gesundheitsbranche mit „Cryptshare for Healthcare“ im Fokus: Im Gesundheitswesen sehen wir einen hohen Bedarf an sicheren und anwenderfreundlichen Lösungen, um die Kommunikation mit Patienten und externen Partnern zu digitalisieren.

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

Wie sieht das konkret in der Praxis aus?

Mit SHD System-Haus-Dresden haben wir hier bereits seit 2011 einen erfahrenen Partner an unserer Seite, der seit fast 30 Jahren erfolgreich IT-Infrastruktur-, IT-Sicherheits- und Digitalisierungs-Projekte im Klinikumfeld umsetzt.

Zusammen konnten wir schon viele Krankenhäuser beraten, auch sehr große mit bis zu 8.000 Mitarbeitern. Diese Partnerschaft möchten wir nun weiter verstärken.



Sie sprachen die SHD gerade an. Wie können Sie mit Ihren Lösungen und dieser Partnerschaft Anforderungen der Krankenhäuser optimal unterstützen?

Dass im Gesundheitswesen tagtäglich große Mengen an vertraulichen Informationen ausgetauscht werden, ist nichts Neues.

Die aus meiner Sicht wichtigste Neuerung in der aktuellen Situation ist, dass nicht nur Krankenhäuser miteinander kommunizieren und vertrauliche Informationen austauschen müssen, sondern ein breites Spektrum an Einrichtungen quer durch den Gesundheitsmarkt bis hin zu den Patienten selbst. Unter Druck, ohne Zeit für komplizierte Installationen. Natürlich ist in diesem Zusammenhang – richtigerweise – viel über virtuelle private Netzwerke gesprochen worden, aber die sind nicht für jeden einfach einzurichten. Unsere Lösung bietet eine schnell zu installierende Alternative, die Sicherheit mit Bedienkomfort vereint, also sichere Kommunikation schnell nutzbar macht.

Generell gibt es aus technischer Sicht verschiedene Ansätze, wie der Austausch sensibler Daten einfach, sicher und gemäß den gesetzlichen Vorschriften erfolgen kann. Damit kann man auch die von E-Mails bekannte Größenbeschränkung überwinden, denn bei größeren Anhängen stoßen E-Mail-Systeme meist sehr schnell an ihre Grenzen.

Wenn sich die Lösung bequem in die Workflows der Mitarbeiter integrieren lässt, kann auch die sogenannte „Schatten-IT" vermieden werden, also der Einsatz nicht autorisierter Software. Und wenn die Lösung auch mobil nutzbar ist, können Ärzte, Pflegepersonal, Praxismitarbeiter und Forscher Daten auch per Tablet oder Smartphone austauschen, ohne auf nicht datenschutzkonforme Dienste wie SMS oder WhatsApp zurückgreifen zu müssen.

Und hier schließt sich der Kreis wieder, denn die SHD kann diese Komplexität mit ihrer langjährigen Erfahrung überblicken, so dass wir gemeinsam erfolgreiche Projekte realisieren können.

Welche Hürden müssen überwunden werden, damit sich die Krankenhaus-IT-Infrastruktur für die Zukunft gerüstet zeigen kann?

Auch hier spielt die DS-GVO eine große Rolle. Ein wichtiger Compliance-Standard, den die Verordnung fordert, ist der adäquate Umgang mit Daten, die unterschiedlich hohen Schutz erfordern. Mit der „E-Mail-Klassifizierung" können medizinische Einrichtungen die gesetzlichen Vorgaben erfüllen und auch eigene Richtlinien umsetzen. Konkret bedeutet das, dass beispielsweise streng vertrauliche Patientendaten zwingend als verschlüsselter Anhang mit einem Einmalpasswort und mit nachvollziehbarer Empfangsbestätigung versendet werden müssen.

Wie kann sich die Healthcare-Branche besser gegen die immer ausgefeilter werdenden Cyberangriffe wappnen?

Im Grunde sind es vor allem drei Dinge, die alle Beteiligten in der Healthcare-Branche angehen müssen: Erstens die Sensibilisierung der Mitarbeiter fördern, zweitens ein effizientes Risikomanagement betreiben und drittens konkrete Maßnahmen ergreifen, die verhindern, dass personenbezogene Daten in die falschen Hände gelangen.

Das ist schon allein im Hinblick auf gesetzliche Regelungen wie die DS-GVO relevant...

Wo sehen Sie aktuell den größten Handlungsbedarf?

Da ist zum einen die Digitalisierung der Kommunikation zwischen Krankenhäusern, Arztpraxen und Patienten zu nennen, Stichwort „digitale Patientenakte". Zum anderen die Eliminierung der Schatten-IT. Fast die Hälfte aller Ärzte haben Umfragen zufolge schon einmal Fotos oder Röntgenbilder mit dem Smartphone versendet. Nur mit einer anwenderfreundlichen Lösung kann der Gebrauch von nicht-autorisierter Software verhindert und so die Nachvollziehbarkeit der digitalen Kommunikationswege sichergestellt werden.

www.cryptshare.com/healthcare

Phishing im Gesundheitswesen: Was kann helfen?

Organisationen im Gesundheitswesen werden mit Phishing-Angriffen geradezu bombardiert. Eine kürzlich durchgeführte Studie des GDV hat gezeigt, dass E-Mails und Phishing immer noch die häufigsten Ursachen für erfolgreiche Angriffe sind. Besonders im Zuge der aktuellen Corona-Krise ist laut einigen Berichten ein verstärktes Aufkommen von Phishing-Mails zu beobachten. Wenn sich Gesundheitsorganisationen mit Phishing befassen, sollten sie verschiedene Methoden anwenden, die die Wahrscheinlichkeit von Phishing-Angriffen zu verringern und den potenziellen Schaden zu minimieren. Die Frage ist jedoch, wie effizient diese Maßnahmen sind und welchen Ansatz Gesundheitsdienstleister verfolgen sollten, um eine Gefährdung sensibler Daten durch Phishing-Angriffe zu vermeiden.

Warum gibt es so viele Phishing-Angriffe auf Gesundheitsorganisationen?

Es gibt mehrere Gründe, warum Phishing-Angriffe auf Gesundheitsorganisationen so häufig vorkommen. Erstens haben sie eine hohe Erfolgsquote. Schließlich ist nur ein einziger Fehler erforderlich – ein Mitarbeiter, der dazu verleitet wird, einen schädlichen Link anzuklicken – damit der Täter in das Organisationsnetzwerk gelangen kann. Außerdem werden einige Phishing-Angriffe, die als Spear-Phishing bezeichnet werden, sorgfältig auf bestimmte Benutzer ausgerichtet. Dies erhöht die Wahrscheinlichkeit, dass sie die E-Mail öffnen und die darin enthaltenen schädlichen Links anklicken.

Schließlich ist die Motivation für Hacker, sich an Gesundheitsorganisationen zu wenden, sehr hoch, da die von ihnen gespeicherten persönlichen Gesundheitsinformationen sehr wertvoll sind. Laut dem Center HYPERLINK "https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/"forHYPERLINK "https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/" Internet Security (CIS) kann eine Krankenakte auf dem Schwarzmarkt für bis zu 335 Euro verkauft werden, personenbezogene Daten hingegen für nur 1 bis 2 Euro. Der Grund für diesen Kostenunterschied ist einfach: Kriminelle können Gesundheitsakten leicht für Betrug, Identitätsdiebstahl oder Erpressung verwenden, und die Opfer können diese Aufzeichnungen nicht annähernd so leicht unbrauchbar machen, wie sie eine Kreditkartennummer stornieren oder ein Bankkonto schließen können.

Wie können Gesundheitsdienstleister die Wahrscheinlichkeit eines erfolgreichen Phishing-Angriffs verringern?

Der erste Schritt zur Abwehr von Phishing-Angriffen besteht darin, umfassende Mitarbeiterschulungen durchzuführen und regelmäßig zu testen, wie gut alle die Lektionen verinnerlicht haben. Viele Gesundheitsorganisationen verstärken ihre Bemühungen in diesem Bereich. In vielen Krankenhäusern ist es bereits üblich, Mitarbeitern die Gefahren von Phishing-Mails näherzubringen und ihnen Leitfäden für den richtigen Umgang mit solchen Nachrichten an die Hand zu geben. Im weiteren Sinne stellte der Bericht von HYPERLINK "https://www.netwrix.com/2020ittrendsreport.html"NetwrixHYPERLINK "https://www.netwrix.com/2020ittrendsreport.html" zu den IT-Trends 2020 fest, dass 56 % der Gesundheitsorganisationen ein besseres Cybersicherheitsbewusstsein zu einer ihrer obersten Prioritäten für 2020 machen.

Der zweite wichtige Schritt ist die Implementierung strengerer Sicherheitsrichtlinien, insbesondere in Bezug auf E-Mail-Sicherheit und Kennwortkomplexität. Erfolgreiche Phishing-Angriffe wie auf das Krankenhaus in Fürstenfeldbruck haben dazu geführt, dass Kliniken und andere Gesundheitsbetriebe ein größeres Augenmerk auf die Sicherheit ihrer E-Mails und Passwörter legen. Organisationen sollten mit der Überprüfung und Aktualisierung ihrer Richtlinien zweifelsohne nicht erst bis nach einem Datenleck warten. Vielmehr gilt es, schnellstmöglich dafür zu sorgen, dass Passwort- und E-Mail-Richtlinien dem Stand der Zeit entsprechen.

Diese Schritte verringern zwar die Wahrscheinlichkeit eines erfolgreichen Phishing-Angriffs, können jedoch keinen 100-prozentigen Datenschutz garantieren. Es besteht immer die Gefahr, dass ein Mitarbeiter einen Moment lang unauf-

merksam ist und auf einen Link in einer Phishing-E-Mail klickt - insbesondere, wenn es sich um eine besonders überzeugende Spear-Phishing-Nachricht handelt.

Darüber hinaus ist Phishing nicht die einzige Bedrohung für Gesundheitsdaten. Ein weiterer wichtiger Faktor sind verdächtige Benutzeraktivitäten in der gesamten IT-Umgebung der Organisation, ob on premis, in der Cloud oder in Hybrid-Umgebungen. Der NetwrixHYPERLINK "https://www.netwrix.com/2019cloudsecurityreport.html" 2019 HYPERLINK "https://www.netwrix.com/2019cloudsecurityreport.html"Cloud Data Security Report stellte fest, dass 49 Prozent der Gesundheitsorganisationen Patientendaten jetzt in der Cloud speichern. Daher ist es für Unternehmen von entscheidender Bedeutung, zu wissen, wo welche Daten gespeichert sind und welchen Grad an Vertraulichkeit sie besitzen. So lässt sich vermeiden, dass hochsensible Informationen wie Krankenakten, Röntgenbilder etc. an unbekannten Speicherorten verschwinden und somit Gefahr laufen, kompromittiert zu werden.

Was sind die besten Methoden, um Patientendaten vor Phishing-Angriffen und anderen Bedrohungen zu schützen?

Organisationen müssen umfassende Benutzerschulungen einleiten und ihre Sicherheitsrichtlinien stärken, um möglichst viele Angriffe zu blockieren. Genauso wichtig ist es allerdings, Maßnahmen zu ergreifen, mit denen sie erfolgreiche Phishing-Angriffe und verdächtiges Benutzerverhalten schnell erkennen und untersuchen können. Wenn sichergestellt ist, dass Hacker aufgehalten werden können, bevor sie große Mengen Patientendaten gefährden, minimieren sich finanziellen Verluste, Compliance-Verstöße und schlechte Reputation. Hier die wichtigsten Best Practices, die Gesundheitsbetriebe implementieren sollten:

Überwachung von Nutzeraktivitäten. Es ist von großer Wichtigkeit, ein besseres Bewusstsein dafür zu erlangen, was in IT-Umgebungen vor sich geht. Dazu gehört auch die Frage, wer welche Daten ändert oder kopiert. Wenn IT-Verantwortliche ungewöhnliche Aktivitäten erkennen, die Patientendaten gefährden könnten und diese unverzüglich untersuchen, können sie Maßnahmen in die Wege leiten, bevor es zu einem Datenleck kommt. Im Idealfall werden die für die IT-Sicherheit zuständigen Mitarbeiter bei verdächtigen Ereignissen gewarnt, zum Beispiel bei mehreren fehlgeschlagenen Anmeldeversuchen oder wenn jemand auf medizinische Informationen zugreift, auf die er zuvor noch nie einen Blick geworfen hat.

Regelmäßige Überprüfung von Privilegien. Ein Hacker, der die Anmeldedaten eines Mitarbeiters kompromittiert, kann auf alle vertraulichen Daten zugreifen, zu denen das Konto Zugang hat. Sicherzustellen, dass jeder Benutzer nur über die absoluten Mindestberechtigungen verfügt, die er für seine Arbeit benötigt, gehört daher zu den grundlegenden Best Practices. Ein Praktikant sollte beispielsweise keinen Zugriff auf vertrauliche Patientendaten haben. Durch die konsequente Durchsetzung des Prinzips der geringsten Privilegien bei regelmäßiger Überprüfung der Berechtigungen lässt sich die Angriffsfläche erheblich reduzieren. Privilegierte Nutzer sollten unter genauerer Beobachtung stehen, da Hacker häufig versuchen, ihre Anmeldedaten zu erlangen. Besonders wichtig ist, dass privilegierte Nutzer keinen universellen Zugriff auf alle Systeme und Datenspeicher haben (beispielsweise sollte ein SQL-Administratorkonto kein Mitglied der Domänenadministratorgruppe sein).

Klassifizierung von Daten. Wenn bekannt ist, welche Daten abgespeichert sind, wo sich diese befinden und wer Zugriff auf sie hat, kann eruiert werden, welche Daten die größte Aufmerksamkeit erfordern. Danach kann man Kontrollen zu ihrem Schutz auswählen. IT-Verantwortliche können eine Datenklassifizierung nutzen, um die Risiken für Gesundheitsdaten zu bewerten und die wertvollsten Daten (etwa Testergebnisse und Diagnosen) nur an sicheren Orten zu speichern. Zugleich ist die Einhaltung von Datenschutzverordnungen wie der EU-DSGVO sichergestellt.

Sonstige Anti-Phishing-Techniken. Um das Risiko eines Datenlecks weiter zu verringern, müssen Gesundheitsorganisationen ihre allgemeine IT-Sicherheit im Auge behalten und gegebenenfalls verbessern. Hierunter fallen zum Beispiel, Software-Patches immer auf dem neuesten Stand zu halten, vertrauliche Daten zu verschlüsseln und Antivirensoftware einzusetzen.

Um Phishing-Bedrohungen effektiv zu bekämpfen und Daten zu schützen, bedarf es einer detaillierten Abwehrstrategie. Zu den Schlüsselelementen gehören regelmäßige Cybersicherheitsschulungen, die Durchsetzung des Grundsatzes der geringsten Privilegien für reguläre Benutzer und Administratoren sowie die Klassifizierung von Daten. Nur so können Betriebe ihre Datenschutzbemühungen priorisieren und gesetzliche Vorgaben einhalten.

Jürgen Venhorst, Country Manager DACH bei Netwrix

Sicherheitssysteme und Netzwerkarchitektur strategisch aufsetzen

Digitalisierung – das Gesundheitssystem muss sich neu erfinden

Die Gesellschaft blickt gerade wie sonst selten auf die Gesundheitsbranche. In der Corona-Krise offenbaren sich die Schwachstellen des Gesundheitssystems – auch in Deutschland. Beim Thema Digitalisierung hängt die Branche deutlich hinter anderen Sektoren zurück. Deshalb sollten schon vor der Krise von der Politik initiierte Maßnahmen, wie die elektronische Patientenakte, die Digitalisierung vorantreiben. Doch wer bei den Schritten in die digitale Welt ohne Absicherung handelt, riskiert bald Opfer eines Cyberangriffs zu werden – sensible Patienteninformationen sind ein beliebtes Ziel. Das zeigt sich auch in Zeiten von Corona: Das Uni-Klinikum im tschechischen Brno, das eines der landesweit größten Covid-19-Testlabore betreibt, wurde durch einen Ransomware-Angriff lahmgelegt. In kritischen Zeiten, wie diesen, eine Katastrophe.

Daten und Geräte: Digitale Angriffsflächen für Cyber-Kriminelle

Natürlich hat die Patientenversorgung im Gesundheitswesen oberste Priorität. Gerade deshalb bleibt aber die IT oft auf der Strecke. Doch veraltete IT-Infrastruktursysteme können großen Schaden anrichten, indem sie den Arbeitsablauf unterbrechen und die Sicherheit und Privatsphäre der Patienten gefährden. Aber nicht nur veraltete Systeme, wie z.B. die noch immer verbreitete Verwendung von Windows XP – noch jedes zehnte Gerät läuft, laut einer Infoblox-Umfrage noch auf diesem System, für das der Support bereits vor über 5 Jahren eingestellt wurde – sondern auch intelligent verbundene Geräte stellen ein großes Risiko dar. Denn das Gesundheitswesen stützt sich zunehmend auf Technologien, die mit dem Internet verbunden sind – von elektronischen Patientenakten bis hin zu radiologischen Geräten. Diese Entwicklungen sind zwar gut für die Qualität der Patientenversorgung, aber die angeschlossenen Geräte sind oft anfällig für Cyber-Angriffe, die sensible Patientendaten abschöpfen, Maschinen oder sogar ganze Gesundheitseinrichtungen abschalten können.

Ein Beispiel: Im Mai 2017 verwüstete der berüchtigte Lösegeldangriff WannaCry Hunderttausende von Computernetzwerken, darunter auch das des britischen NHS. Im Gegensatz zu den meisten großen E-Mail-Angriffen konnte WannaCry durch Netzwerk-Schwachstellen in Organisationen eindringen, was dazu führte, dass mehr als 19.000 Termine abgesagt und 200.000 Computer ausgesperrt wurden und dem NHS über 92 Millionen Pfund Schaden zugefügt wurde. Dieser verheerende Angriff war sicherlich ein Weckruf für Gesundheitsorganisationen, ihre Systeme neu zu bewerten.

Vorbeugen ist die beste Lösung

Auch wenn die IT-Verantwortlichen seit 2017 im Gesundheitswesen Maßnahmen ergriffen haben, um ähnliche Angriffe in Zukunft abzuschwächen, so sind Daten aus dem Gesundheitswesen im Dark Net so wertvoll wie eh und je. Deshalb müssen Organisationen im Gesundheitswesen ihre IT-Sicherheit stets weiterentwickeln. Automatisierte Systeme sind dabei sehr hilfreich, denn sie scannen die Netzwerke aktiv auf verdächtige Aktivitäten. Zusätzlich sollten größere Organisationen spezielle Sicherheitsoperationszentren einrichten, in denen die Security-Maßnahmen gebündelt laufen und überwacht werden. Ransomware-Attacken, bei denen IT-Systeme lahmgelegt werden und Lösegeld erpresst wird, sind weit verbreitet. So legte der Trojaner Emotet Ende 2018 das Krankenhaus Fürstenfeldbruck für ca. eine Woche komplett lahm: Die Telefonanlage fiel aus, Rettungswägen wurden umgeleitet, Blutproben wurden von Hand beschriftet. Krankenhäuser sollten deshalb auf jeden Fall einen Plan entwickeln, um im Falle eines solchen Angriffs handlungsfähig zu sein. Das Bezahlen des Lösegeldes sollte dabei keine Option sein. Die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik HYPERLINK "https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3"(BSI) zeigen, wie in solch einer Situation gehandelt werden sollte.

Generell gilt: Wer sich im Vorfeld von Cyberattacken gut aufstellt, kann den betriebswirtschaftlichen Schaden, der bei einem Angriff entsteht, gering halten. Auch wenn die Herausforderungen für eine zeitgemäße Sicherheitsstrategie groß

sind – die Implementierung lohnt sich. Folgende Maßnahmen sind ein guter Ansatzpunkt:

- Die Schulung und Aufklärung von Mitarbeitern ist das A und O. Oft ist es ein simpler, unüberlegter Klick auf einen Link, der das Einfallstor für Cyberkriminelle öffnet.
- Regelmäßiges patchen und aktualisieren der IT-Systeme mag banal klingen, ist aber längst keine Selbstverständlichkeit.
- Allein der Überblick, welche Geräte sich im Netzwerk befinden, kann helfen Eindringlinge zu entlarven. Leider tappen hier viele im Dunkeln.
- Der Flickenteppich an Security-Lösungen muss stärker in Fokus der IT-Verantwortlichen gerückt werden. Viele Lösungen arbeiten inselartig nebeneinander. Netzwerk- und Sicherheitstools müssen in Einklang gebracht und automatisiert werden, um bei hochkomplexen Angriffen effektiv zu arbeiten.

Umstieg auf die Cloud: Herausforderungen fürs Netzwerk-Management

Doch IT-Verantwortliche sind nicht nur in Sachen Security stark gefordert. Auch die Netzwerk-Architektur befindet sich im digitalen Umbruch. Mit der Entwicklung des Gesundheitswesens hin zu immer größeren Klinikbetreibern mit Niederlassungen in der ganzen Republik, ist die Gesundheitsbranche zunehmend auf Cloud-gehostete Dienste, wie Office 365, zur Verwaltung kritischer Arbeitslasten umgestiegen. Traditionellen WAN-Architekturen stoßen damit an ihre Grenzen. Doch aktuell ist die Netzwerk-Zuverlässigkeit an dezentralen Standorten verbesserungsfähig. Eine InfobloxHYPERLINK "https://www.infoblox.com/wp-content/uploads/infoblox-whitepaper-remote-office-networks-pose-business-and-reliability-risk-survey.pdf"-Umfrage aus dem Jahr 2019 ergab, dass bis zu 75 % der Netzwerk-Administratoren mehrmals im Jahr oder öfter Netzwerkunterbrechungen erleben. Eine schlechte Konnektivität kann erhebliche Auswirkungen auf den Rest des Unternehmens haben, wobei fast alle (99%) der Befragten von negativen Auswirkungen berichten. Ausfallzeiten von mehr als 3 Stunden sind dabei keine Seltenheit. Software-Defined WAN (SD-WAN) kann eine einfache und kostengünstige Möglichkeit sein, Gesundheitsorganisationen eine zuverlässige und optimierte Konnektivität zu den Cloud-basierten Anwendungen zu bieten.

Sinnvolle Netzwerkarchitektur

Damit SD-WAN nicht scheitert, ist es wichtig, dass auch zugrunde liegende Namensauflösung und Adressvergabe (DDI) ebenfalls modernisiert werden. Hinter dem Begriff DDI verbirgt sich DNS, DHCP und IP-Adress-Management. DDI ist eine entscheidende Komponente für Netzwerkverbindungen, sei es im Rechenzentrum oder in der Niederlassung. Zu oft setzen Unternehmen jedoch SD-WAN ein, ohne sich Gedanken darüber zu machen, wie sich ihre DDI-Plattformen ebenfalls verbessern können. Für einen performanten Einsatz von SD-WAN sollte deshalb auch Cloud verwaltetes DDI in den Niederlassungen implementiert werden.

Die Vorteile auf einen Blick:

- Verbesserte Endnutzerfreundlichkeit: Die lokale DNS-Namensauflösung von Endpunkten ermöglicht, dass die nächstgelegenen Einstiegspunkte für SaaS-Anwendungen verwendet werden. Dies führt zu einer schnelleren Reaktionszeit.
- Zuverlässigkeit auf Unternehmensebene: Durch die Verlagerung der Steuerungs- und Verwaltungsfunktionen in die Cloud, wird eine einfache virtuelle Appliance vor Ort bereitgestellt. Dies gewährleistet kürzere Reaktionszeiten.
- Cloud Managed Automation: Zero-Touch-Provisioning automatisiert die Bereitstellung tausender Remote-Standorte und bietet eine zentralisierte Richtlinienkontrolle - ohne fehleranfällige manuelle Methoden für jeden Standort.
- Damit erhalten Unternehmen in der Gesundheitsbranche eine flexible, skalierbare und zuverlässige Plattform, die dazu beiträgt, IT-Dienstleistungen überall zu vereinfachen. So können Organisationen im Gesundheitswesen die Vorteile von SD-WAN voll auszuschöpfen.
- Die Digitalisierung zwingt die Gesundheitsbranche, fest etablierte Strukturen zu hinterfragen. Security und Netzwerkarchitektur sollten dabei eine zentrale Rolle spielen. So werden zum einen sensible Daten geschützt und zum anderen die IT – und damit letztendlich der gesamte Betrieb – am Laufen gehalten. Die Herausforderungen werden dabei nicht weniger. Aber eine zukunftsgerichtete Netzwerk- und Security-Struktur ist für ihre Bewältigung eine wichtige Basis.

Felix Blank, Senior Manager,
Pre-Sales Systems Engineer bei Infoblox

Wir trauern um Hartmuth Wehrs

Nachruf

Mit tiefer Trauer teilen wir mit, dass Hartmuth Wehrs, Gründer und Geschäftsführer der Antares Computer Verlag GmbH, im Alter von 72 Jahren, nach kurzer, aber schwerer Krankheit, am Freitag, dem 15. Mai 2020, verstorben ist.

Bereits Ende der 80er Jahre war Herr Wehrs als Journalist für verschiedene Fachpublikationen aktiv und brachte als Experte die Bereiche Medizin und EDV zusammen.

Im Jahr 1993 war er Mitbegründer des Antares Verlages, der mit seiner Publikation "Computer-Führer für Ärzte" das Standardwerk für niedergelassene Ärzte bei der Beschaffung eines EDV-Systems herausbrachte.

1998 gründete er den Antares Computer Verlag in Dietzenbach und erweiterte das Portfolio auch um das stationäre Gesundheitswesen.

Seit dem Jahr 2002 brachte Hartmuth Wehrs die Fachzeitschrift Krankenhaus-IT Journal heraus, eine Zeitschrift, die bis heute als meinungsbildende Fachzeitschrift der Branche gilt.

Hartmuth Wehrs war als Autor zahlreicher Bücher, Publikationen und Fachzeitschriften mehr als 30 Jahre in der Branche unterwegs und galt stets als gut unterrichteter Experte für alle IT-Themen in der Medizin.

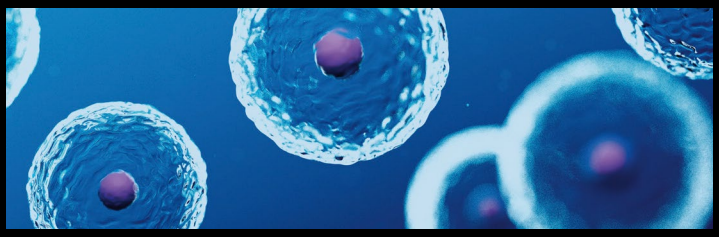
Im Jahr 2019 erschien mit dem Buch "Die Geschichte der Health-IT" ein mehr als 500 Seiten umfassender Rückblick auf 50 Jahre Health-IT in Deutschland.

Das Buch bezeichnete er selbst gerne als seine Memoiren.

Bis ins Jahr 2020 war Hartmuth Wehrs im Berufsleben aktiv, zuletzt beratend für seine beiden Söhne Kim und Kai, die den Verlag seit 2019 führen.

Wir werden seine Expertise, seine kollegiale und freundliche Art sehr vermissen.
Wir möchten sein Lebenswerk weiterführen und werden ihn immer in guter Erinnerung behalten.

Verbinden Sie die Gesundheits-IT von heute mit den Digitalisierungs-lösungen von morgen.



- **Gesundheitsinformationen**
  HealthShare Lösungen
- **Gesundheitsnetze aufbauen**
  Unified Care Record
- **Gesundheitsdaten analysieren**
  Health Insight
- **Gesundheitsdaten vernetzen**
  Health Connect
- **Patienten einbinden**
  Personal Community

ZUM ZWEITEN MAL IN FOLGE AUSGEZEICHNET

Gartner peerinsights customers' choice 2020™

"Professionell und Kundenorientiert."

https://www.intersystems.com/de/customers-choice/

www.InterSystems.de/healthshareproduktfamilie

InterSystems® HealthShare

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