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

Ausgabe 2 / 2020

Krankenhaus-IT JOURNAL

Fakten und Perspektiven der IT im Gesundheitswesen

KRITISche Zeiten im Krankenhaus

Ist die IT der Rettungsanker ?

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

KRITIS in der Krise

Für Betreiber Kritischer Infrastrukturen (KRITIS) ist die Ausbreitung von Covid-19 eine Herausforderung. Ihre Fach- und Führungskräfte sind in diesen Tagen durch Krise und KRITIS besonders gefordert.
Seit der globalen Verbreitung von COVID-19 ist die Welt in Alarmbereitschaft. Nach dem ersten Bericht über das neue Coronavirus (2019-nCoV) in Wuhan/China steigen die Zahlen der bestätigten Fälle und Todesfälle weltweit an. Da keine spezifische Behandlung oder ein Impfstoff zur Verfügung stehen, erklärte die Weltgesundheitsorganisation den öffentlichen Gesundheitsnotstand zum internationalen Problem. Die globalen und wirtschaftlichen Auswirkungen des Virus sind massiv. Es heißt vorsorgen und schnell reagieren.

In außergewöhnlichen Situationen müssen grundlegende Aufgaben bei der Versorgung der Bevölkerung wahrgenommen werden. Für Betreiber Kritischer Infrastrukturen im Gesundheitswesen heißt das: Um jetzt arbeitsfähig zu bleiben ist das betriebliche Krisenmanagement gefragt. Dessen Ziele sind: die bestmögliche Aufrechterhaltung der Funktionsfähigkeit Kritischer Infrastrukturen bzw. der schnellstmögliche Wiederanlauf der kritischen Prozesse nach einer Störung.

Unternehmen in der Krisenbewältigung haben ihre Krisenorganisation aktiviert. Das heißt: Alle relevanten Aufgaben und konkrete Entscheidungsbefugnisse sind im Krisenmanagement festgelegt (Lagefeststellung und -beurteilung, Entscheidung und Kontrolle) und konkreten Personen und deren Vertretungen zugewiesen. Alle Beschäftigten sind hinsichtlich eines verantwortungsvollen Verhaltens und Gefahren während einer Pandemie am Arbeitsplatz und auch im privaten Umfeld informiert. Alle Beschäftigten sind über die Krisenorganisation und die damit verbundenen Änderungen in der Ablauforganisation informiert.

Das Schlüsselpersonal für Kernprozesse ist identifiziert und Ersatzpersonal steht zur Verfügung.

Die Pläne für eine kontrollierte Stilllegung des Betriebes sind für den Fall aktualisiert, dass ein grundlegender Personalmangel eintritt. Entscheidungen des Krisenmanagements werden dokumentiert und für die Nachbereitung der Krisenbewältigung vorgehalten.

Anforderungen an IT-Experten steigen bei Strategie, Konzeption und Umsetzung. IT-Sicherheit beim Zusammenspiel von Informations- und Kommunikationswesen sowie auch Medizintechnik ist Kernkompetenz. Denn Cyberkriminelle machen sich das erhöhte Informationsbedürfnis in der aktuellen Lage zunutze. Sie verbreiten schädliche Links und manipulierte Anhänge mit Schadsoftware. Auch in Deutschland sind spezifische COVID-19-Mails im Umlauf.

Die Corona-Pandemie zeigt, wie wichtig der Stellenwert von Sicherheit bei der Digitalisierung ist. Egal ob in Krankenhäusern oder anderen Branchen, erfolgreiche Cyber-Zwischenfälle hatten überwiegend die Schwachstelle „Mensch" als Ursache. Hier helfen regelmäßige Awareness-Maßnahmen der Mitarbeiter heilen.

Bleiben Sie gesund!
Herzliche Grüße, Wolf-Dietrich Lorenz

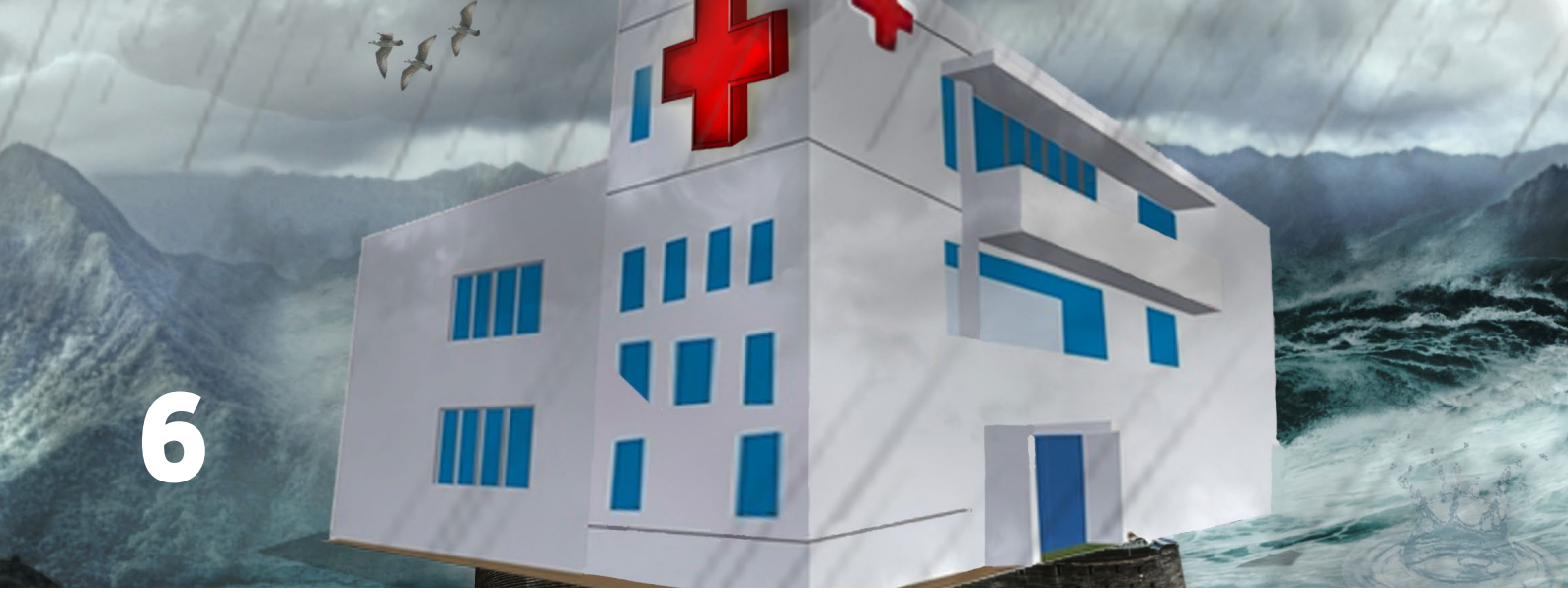
Dagmar Finlayson

Hartmuth Wehrs

Kim Wehrs

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

Fotonachweis
S. 6, 8, 20, 24, 38, 67, 69, 73
Adobe Stock;
S. 11 BSI; S. 12, 13 x-tention;
S. 18, 19 Klinikum Höchst;
S. 30, 31 PwC; S. 36 Bayoonet;
S. 49, 50 kw; S. 53, 54 wdl;
S. 56,57 Entscheiderfabrik;
S. 58, 59 Agfa HealthCare;
S. 60, 61 Lahn-Dill-Kliniken;
S. 62, 63 Heidelberg Eye Explorer;
S. 64, 65 SAS;
S. 66 Zerto;
S. 75, 76, 77 Kaspersky



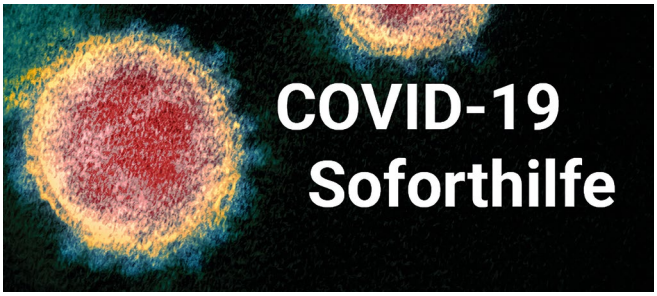
6

Titelthema

KH IT Frühjahrstagung

IT-Management

Verbandsseiten KH-IT



Veranstaltungen

Aus dem Markt

IT-Sicherheit im Krankenhaus

Status und Perspektiven für das Gesundheitswesen

Wo der *KRITIS-Schuh* drückt

Die Digitalisierung des Gesundheitswesens ist eines der zentralen Zukunftsthemen für die Krankenhäuser in Deutschland. Sicherheit bei intersektoraler Vernetzung von Gesundheitseinrichtungen, elektronischen Fall- und Patientenakten, Anwendungen der Telemedizin, Big Data, der Nutzung mobiler Endgeräte sowie der Transformation von Prozessen eröffnen Chancen für eine bessere und effizientere Versorgung der Patienten. KRITIS – das geht jeden Betreiber an, ob groß oder klein. Von *Wolf-Dietrich Lorenz*

Das Corona-Virus bringt das Gesundheitssystem an das Limit. Dabei kann die Digitalisierung für die Gesundheitsversorgung neue Chancen eröffnen. Die IT im Krankenhaus beschleunigt geradezu rasant in das digitale Zeitalter hinein. Was sonst langwieriger Überlegungen und zahlreicher Arbeitsgruppentreffen bedurfte, scheint nun schnell von der Hand zu gehen: Webkonferenzen für alle, Videosprechstunde in den Ambulanzen und eine Mitarbeiter-App als Ergänzung zu althergebrachten Rundmails und Intranet. Anträge auf Home Office, Laptop und Webcam-Ausstattung haben Hochkonjunktur. Die Komplexität der stationären sowie mobilen IT-Welt nimmt dadurch rapide zu. Die Anforderungen an die IT-Experten steigen – bei Strategie, Konzeption und Umsetzung. Das betrifft besonders die IT-Sicherheit im Zusammenspiel von Informations- und Kommunikationswesen sowie auch Medizintechnik.

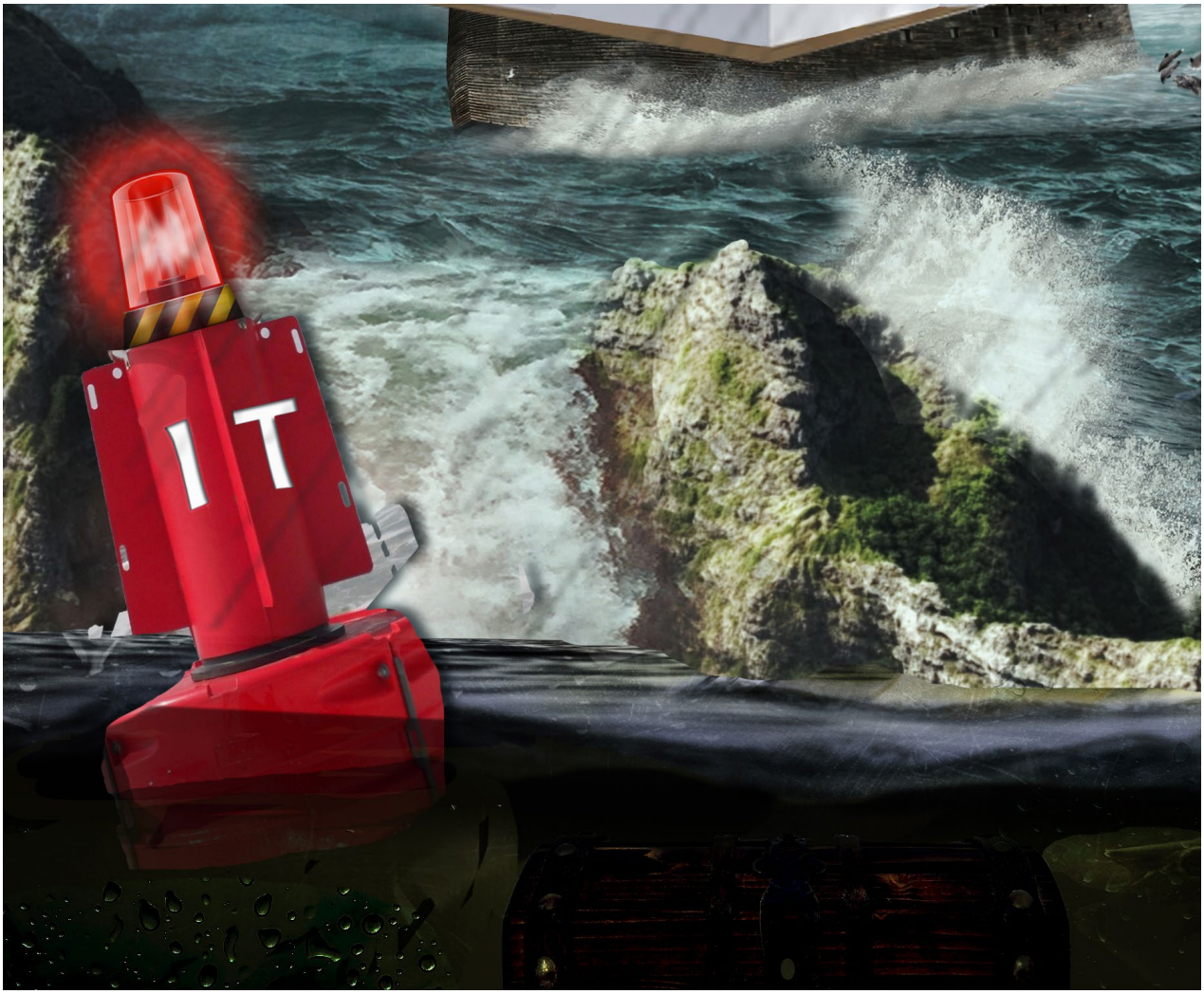
Wachmacher

Hier rückt unübersehbar KRITIS in den Blick. Dabei kann die Umsetzung der Anforderungen das Bewusstsein schärfen. Die Anwendung des Branchenstandards B3S vereinheitlicht zudem die Abläufe und das Denken und ermöglicht den Austausch der KRITIS-relevanten Krankenhäuser untereinander. Indem Krankenhäuser Prozesse von Anfang bis zum Ende durchdenken, um im Anschluss ein ISMS zu implementieren, schaffen sie die Voraussetzung, mit der zunehmenden Digitalisierung im Gesundheitswesen aus Sicht der Cybersicherheit Schritt zu halten. (Lesen Sie dazu „KRITIS – Befund und Prognose - Wachmacher für die Krankenhäuser“auf Seite 24.)

Wissensmanagement

Ist auch die IT im Krankenhaus nach eigener Einschätzung oft bis an die Grenzen ausgelastet, ist eine Auslagerung von Kompetenzen immer zu überlegen. Zwar wird es wohl kaum das eine Multi-Talent geben, das alle Prozesse in einem Krankenhaus vollständig kennt. „Stattdessen ist eine Abteilung gefragt, die erhebend und moderierend das Prozesswissen zahlreicher Beteiligter zusammenträgt und in eine sinnvoll aufbereitete Form überführt.“ (Lesen Sie dazu „KRITIS-Erfahrungen - Was der IT-Leiter meint“ auf Seite 20.)

Digitalisierung zeigt sich in verschiedenen Facetten. Sie bestimmt neben Kosteneinsparungen und Personalmangel wesentliche Trends im deutschen Gesundheitswesen. Dies gilt sowohl vor dem Hintergrund interner Maßnahmen und IT-Projekte als auch angesichts der fortschreitenden Digitalisie-



rung der Gesellschaft. Innerhalb der eigenen Organisation ist entsprechende Initiative vor allem deshalb unumgänglich, damit künftig mehr denn je ein Klinikbetrieb gewährleistet werden kann, der qualitativ und unter Effizienzgesichtspunkten überzeugt. Ebenfalls gefordert ist Kontrolle der Gesundheitseinrichtungen, wenn es darum geht, die noch zahlreichen Sicherheitslücken im Zusammenspiel von Technik, Informationswesen und Kommunikation zu schließen. Die Umsetzung benötigt vor allem Zeit, und dies ist abhängig von den Ressourcen. (Lesen Sie dazu auch Kampf um Sicherheit, Ordnungsmäßigkeit, Wirtschaftlichkeit - KRITIS: Herausforderung für Krankenhäuser ist die Umsetzung auf Seite 23.)

Audits

Audits sind die Nagelprobe. Geprüft wird dabei zunächst einmal, ob und wie ein kontinuierlicher Verbesserungsprozess in den Schritten Planen – Umsetzen – Prüfen – Aktualisieren / Verbessern eingeführt ist. Dieser Prozess ist der unverhandelbare Kern der ISO 27001 und damit auch des Branchenstandards. Auditor beobachten, dass der KRITIS-Zwang häufig tatsächlich zu einer kontinuierlichen Verbesserung führt. (Lesen Sie dazu „KRITIS-Audits: Es geht um Glaubhaftigkeit - Empfehlungen aus der Sicht des Auditors“ auf Seite 26.)

Schwachstellen

Mit zunehmender IT-Durchdringung wächst die Gefahr, dass nicht allein Krankenhausprozesse durch Ausfälle oder Störungen der IT erheblich beeinträchtigt werden. Computer-Experten befürchten, dass mittlerweile auch Medizingeräte, die in ein Krankenhausnetz integriert sind, eine besondere Anfälligkeit gegen Computerviren aufweisen. Mögliche Bedrohungen offenbaren jene Schwachstellen, die das Eintreten von Sicherheitsvorfällen begünstigen, wie etwa veraltete Technik, unzureichende Schutzmechanismen, unterbliebene Tests von Notfallmaßnahmen oder die Unzufriedenheit von Mitarbeitern.

Der KRITIS-Schuh drückt nicht allein bei der Technik. Egal ob in Krankenhäusern oder anderen Branchen, die meisten erfolgreichen Zwischenfälle hatten überwiegend die Schwachstelle „Mensch“ als Ursache. An erster Stelle muss in jedem Krankenhaus und Unternehmen die regelmäßige Mitarbeiter-Awareness zur Informationssicherheit stehen. Sämtliche bisher vorhandene Schwachstellen stehen mit dem menschlichen Handeln in Verbindung. (Lesen Sie dazu „An erster Stelle bei KRITIS steht die Mitarbeiter-Awarenes - Informationssicherheit gehört automatisch in alle Krankenhausprozesse“ auf Seite 22)

Definition „vollstationär“

Wie wird die relevante Anzahl der vollstationären Fälle ermittelt/berechnet? Die BSI-Kristisverordnung verweist im Hinblick auf die Anlagenkategorie "Krankenhaus" auf § 108 SGB V. Anknüpfungspunkt für die Identifikation des Standortes und der Betriebsstätten eines Krankenhauses im Sinne der Verordnung ist damit die (Landes-)Krankenhausplanung. Die BSI-Kritisverordnung definiert die Anlagenkategorie "Krankenhaus" als "Standort oder Betriebsstätte eines nach § 108 des Fünften Sozialgesetzbuches […] zugelassenen Krankenhauses […]" (siehe Anhang 5, Teil 1 Nr. 1a BSI-KritisV). Die Definition beinhaltet also zwei alternative Tatbestände:

1. "Ein Krankenhaus ist der Standort eines nach § 108 […] zugelassenen Krankenhauses." und
2. "Ein Krankenhaus sind die Betriebsstätten (und zwar alle) eines nach § 108 […] zugelassenen Krankenhauses.".

Im Falle von Nummer 2 sind alle Betriebsstätten, die im Sinne des (jeweiligen) Landeskrankenhausplans als ein Krankenhaus behandelt werden, in Anwendung der Verordnung als eine Anlage zu betrachten. In diesem Fall sind die vollstationären Fälle der einzelnen Betriebsstätten zu summieren. Diese Berechnungsbasis steht dabei in keinem weiteren Zusammenhang mit den IK-Nummern. Bitte prüfen Sie auf dieser Basis die Anzahl der ggf. zu kumulierenden, stationären Fälle.

Anlage

Ist ein Standort oder ein Betriebsstandort eine Anlage? Die BSI-KritisV identifiziert Anlagen als Kritische Infrastrukturen im Sinne des BSIG, keine Standorte. Der Betriebsstandort kann indes ein tatsächliches Kriterium bei der Bewertung sein, ob es sich um eine sog. gemeinsame Anlage i. S. der BSI-KritisV handelt. Daraus folgt aber nicht, dass ein Betriebsstandort in Gänze als Kritische Infrastruktur i. S. d. BSI-KritisV gilt. Maßgeblich sind insoweit ausschließlich die in den Anhängen benannten Voraussetzungen für das Vorliegen einer gemeinsamen Anlage.

Gemeinsame Leitung

Was ist mit "gemeinsamer Leitung" im Zusammenhang mit der Feststellung, ob eine gemeinsame Anlage vorliegt, gemeint? Der Begriff der gemeinsamen Leitung bezieht sich nicht auf physikalische Steuer- oder Leiteinrichtungen, sondern gewährleistet, dass zwei Anlagen nur dann als gemeinsame Anlage gelten, wenn diese einem Betreiber unterstehen (Grundsatz der Betreiberidentität). Die Voraussetzung ist unproblematisch gegeben, wenn die Anlage von einer (natürlichen oder juristischen) Person betrieben wird. Ein gemeinsames Management, das beide Anlagen führt, spricht somit für eine gemeinsame Leitung im Sinne der Verordnung. Die Voraussetzung ist aber auch dann gegeben, wenn mehrere Anlagen unterschiedlichen juristischen Personen zuzurechnen sind, diese aber in einem konzernrechtlichen Abhängigkeitsverhältnis zueinander stehen.

Verantwortung

Krankenhäuser und andere medizinische Einrichtungen waren zuletzt wiederholt Betroffene gravierender IT-Sicherheitsvorfälle. Neben der Bedrohung durch Ransomware-Angriffe standen dabei auch sensible Patientendaten im Mittelpunkt. Nun hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Eignung eines branchenspezifischen Sicherheitsstandards (B3S) festgestellt, mit dem Krankenhäuser ihre IT-Sicherheitsmaßnahmen nach dem Stand der Technik ausrichten können. Vorgelegt wurde der B3S von der Deutschen Krankenhausgesellschaft (DKG).

"Krankenhäuser und viele andere Einrichtungen des Gesundheitswesens tragen in mehrfacher Hinsicht eine besondere Verantwortung für ihre IT-Netzwerke. Der Schutz sensibler Patientendaten muss ebenso zuverlässig gewährleistet sein wie die Versorgung von Patientinnen und Patienten mit Unterstützung modernster Computertechnologie. Vor diesem Hintergrund bietet der branchenspezifische Sicherheitsstandard wichtige Rahmenbedingungen, unter denen die Cyber-Sicherheit im Gesundheitswesen weiter erhöht werden kann. IT-Sicherheitsvorfälle wie der erfolgreiche Ransomware-Angriff auf eine Krankenhaus-Trägergesellschaft in Rheinland-Pfalz müssen der Vergangenheit angehören", betont BSI-Präsident Arne Schönbohm.

Etwas weniger als zehn Prozent der Krankenhäuser in Deutschland sind beim BSI als Kritische Infrastrukturen (KRITIS) im Sinne des IT-Sicherheitsgesetzes registriert. Der anerkannte B3S steht auch den vielen kleineren Kliniken, die (noch) nicht zu den „30000er KRITIS-Betreiber“ zählen, zur Verfügung für die Umsetzung angemessener IT-Sicherheitsmaßnahmen. (Lesen Sie dazu KRITIS-Sektor Gesundheit: Kritische Dienstleistungen systematisch schützen - Investition in die Funktionsfähigkeit der medizinischen Versorgung auf Seite 10.)

Sanktionen

Der Entwurf zum IT-SiG 2.0 sieht bei Nichterfüllung der KRITIS-Anforderungen Sanktionen gleichlautend zur DSGVO vor. Damit würde sich der Blick auf notwendige Investitionen verändern und die Bewertung der Wirtschaftlichkeit von Maßnahmen auf ein neues Fundament stellen. Für Einrichtungen, die trotz angedachter Schwellenwerte (noch) nicht zu einer Kritischen Infrastruktur werden, drohten bei Nichterfüllung zwar keine Sanktionen durch die Aufsichtsbehörde, möglicherweise aber auf zivil- oder strafrechtlichem Wege, wenn sie im Falle einer Schädigung von Patienten den Nachweis schuldig bleiben, dem aktuellen Stand der Technik entsprochen zu haben. ***wdl***

Investition in die Funktionsfähigkeit der medizinischen Versorgung

KRITIS-Sektor Gesundheit: Kritische Dienstleistungen systematisch schützen

Wie können Krankenhäuser Informationssicherheit zielgerichtet und systematisch umsetzen? Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannte „Branchenspezifische Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus“ (B3S) bietet konkrete Empfehlungen, die nicht nur für regulierte KRITIS-Betreiber, sondern auch für kleinere Kliniken hilfreich sind.

Von Arne Schönbohm, Präsident des BSI

Krankenhäuser und viele andere Einrichtungen des Gesundheitswesens tragen in mehrfacher Hinsicht eine besondere Verantwortung für ihre IT-Netze. Der Schutz sensibler Patientendaten muss ebenso zuverlässig gewährleistet sein wie die Versorgung von Patientinnen und Patienten mit Unterstützung modernster Computertechnologie. Öffentlich bekannt gewordene IT- Sicherheitsvorfälle wie im Lukaskrankenhaus Neuss, in Krankenhäusern in Rheinland-Pfalz und im Saarland, der Uniklinik Gießen oder dem Krankenhaus Fürstenfeldbruck zeigen, dass medizinische Einrichtungen gezielt und ungezielt Opfer eines Cyber-Angriffs werden können.

Medizinische Versorgung als kritische Dienstleistung

Der Sektor Gesundheit ist von zentraler Bedeutung für das Funktionieren des Gemeinwesens und gehört deshalb zu den Kritischen Infrastrukturen. Bisher sind kritische Dienstleistungen in der stationären medizinischen Versorgung, Versorgung mit Arzneimitteln, Blut- und Plasmakonzentraten sowie lebenserhaltenden Medizinprodukten und die Laboratoriumsdiagnostik über das BSI-Gesetz (BSIG) reguliert, vorausgesetzt die jeweiligen Anlagen überschreiten die derzeit gültigen Schwellenwerte gemäß BSI-KRITIS-Verordnung (BSI-KritisV).

Aktuell erreichen rund zehn Prozent der Krankenhäuser in Deutschland den Schwellenwert von 30.000 vollstationären Fällen pro Jahr und sind damit Betreiber Kritischer Infrastrukturen. Dies verpflichtet sie, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen und dies alle zwei Jahre nachzuweisen. Aber auch viele kleinere Kliniken, die derzeit nicht reguliert sind, nehmen ihre Verantwortung in Bezug auf ihren Versorgungsauftrag sehr ernst und engagieren sich, um ihre Informationssicherheit stetig auszubauen.

Herausforderungen erkennen und neue Aufgaben bewältigen

Nicht nur aufgrund der gesetzlichen Regulierung sehen sich die Krankenhäuser auf dem Gebiet der Informationssicherheit mit Herausforderungen konfrontiert. Kliniken verfügen in der Regel über eine Vielzahl von IT-Anschlüssen, 30.000 Endgeräte sind keine Seltenheit. Durch Digitalisierungsprojekte kommen zahlreiche vernetzbare IT- und Medizin-Geräte hinzu bei gleichzeitiger Nutzung von (oft nicht mehr gepflegten) Altsystemen. Zudem sind Krankenhäuser in der Regel offene Einrichtungen, Zutrittsbeschränkungen lassen sich höchstens für den OP- oder Verwaltungsbereich realisieren. Oft gibt es auch Nachholbedarf, was die Sensibilisierung des Klinikpersonals im Umgang mit den vorhandenen Cyber-Risiken anbetrifft.

Das BSI als nationale Cyber-Sicherheitsbehörde des Bundes steht im regelmäßigen Austausch mit den KRITIS-Betreibern und anderen Akteuren des Gesundheitswesens. Aus den verpflichtenden Meldungen von IT-Störungen und Nachweisen, sowie nicht zuletzt aus den vertrauensvollen Gesprächen mit den Betreibern im Rahmen der KRITIS-Betreuung wird deutlich, dass bereits eine Menge Arbeit in die Erfüllung dieser Aufgaben geflossen ist und Vieles erreicht wurde.

Zielgerichtet und ganzheitlich: Kritische Dienstleistung im Fokus

Um die Informationssicherheit auch weiterhin wirksam zu steigern, lohnt sich ein ganzheitlicher Ansatz. Basis für ein erfolgreiches Informations-Sicherheits-Management-System (ISMS) sind eine IT-Sicherheitskonzeption (Definition von KRITIS- und IT-Schutzzielen, Schutzbedarfsfeststellung, Risikoanalyse etc.) und die betreiberindividuelle Definition des Geltungsbereichs (Scope).

Erfahrungen aus der Praxis zeigen, dass es besonders hilfreich ist, dabei die kritische Dienstleistung gemäß BSI-KritisV in den Blick zu nehmen. Der Prozess der stationären medizinischen Versorgung, bestehend aus den Teilprozessen Aufnahme, Diagnose, Therapie, Pflege und Entlassung, wird so

Netzwerke schützen Netzwerke

Das BSI als Cyber-Sicherheitsbehörde des Bundes unterstützt Krankenhäuser und andere Akteure im Gesundheitssektor mit einer Vielzahl von kostenfreien Angeboten.

UP KRITIS:
Diese Vernetzungsplattform ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Die beteiligten Organisationen arbeiten auf Basis gegenseitigen Vertrauens zusammen. Sie tauschen sich untereinander aus und lernen voneinander im Hinblick auf den Schutz Kritischer Infrastrukturen.
www.kritis.bund.de

Bei Fragen rund um KRITIS können sich Interessierte, z.B. die IT-Sicherheitsbeauftragten aus den Krankenhäusern, an das KRITIS-Büro im BSI unter **kritis-buero@bsi.bund.de** wenden.

Allianz für Cyber-Sicherheit:
Teilnehmer dieser Unternehmensplattform des BSI profitieren von der Expertise des BSI und der Kooperationspartner aus Wirtschaft und Forschung, dem vertrauensvollen Erfahrungsaustausch mit anderen Unternehmen und den exklusiven, für Teilnehmer kostenfreien Angeboten zum Ausbau der Sicherheitskompetenz in Unternehmen.
www.allianz-fuer-cybersicherheit.de

Nationales IT-Lagezentrum:
Mit dem Nationalen IT-Lagezentrum steht das BSI allen Krankenhäusern, ihren Trägern und den zuständigen Stellen in den Ländern als kompetente Anlaufstelle in Notfällen zur Verfügung; auch für Kliniken, die unterhalb der Schwellenwerte nach BSI-KritisV liegen.

zur Richtschnur einer systematischen Planung und Umsetzung von zielgerichteten Maßnahmen im Rahmen des ISMS.

„Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus“ bietet konkrete Orientierung

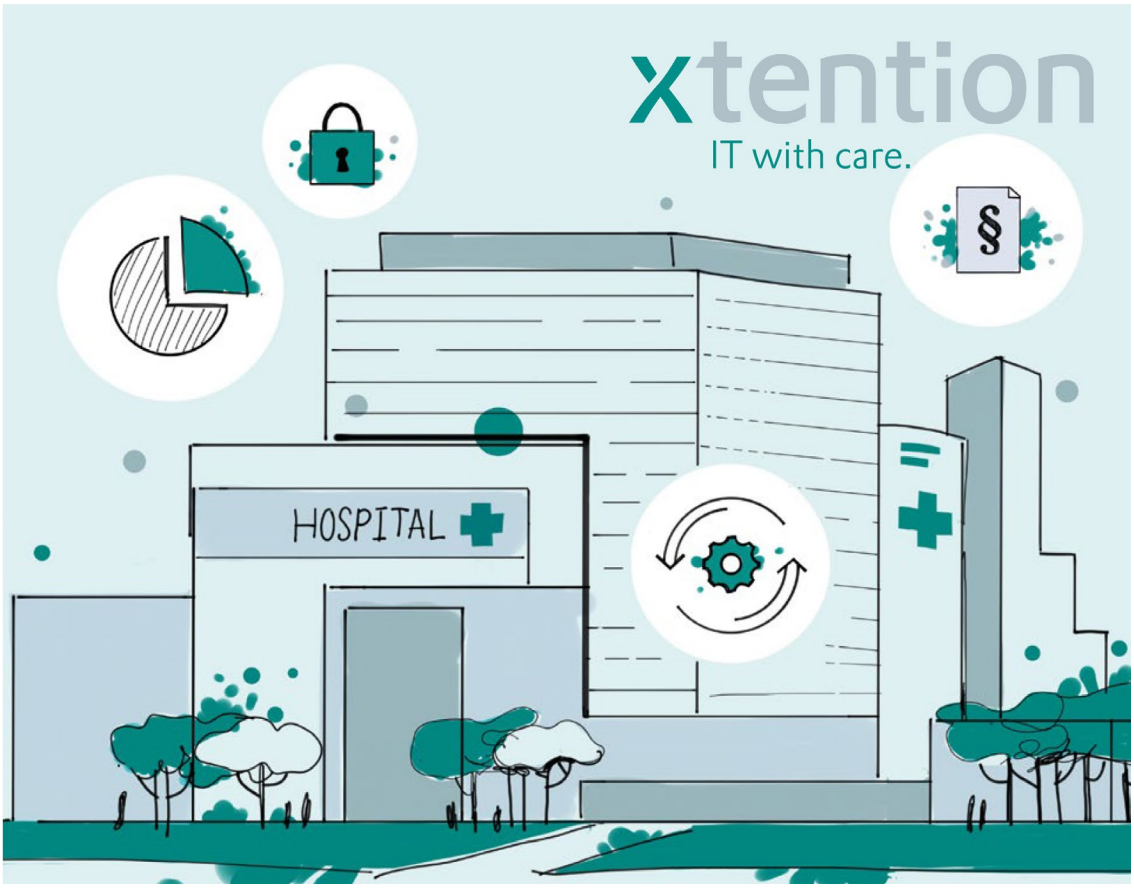
Das BSI hat im Oktober 2019 die Eignung eines branchenspezifischen Sicherheitsstandards (B3S) festgestellt, mit dem Krankenhäuser ihre IT-Sicherheitsmaßnahmen nach dem Stand der Technik ausrichten können. Entwickelt wurde der Standard von engagierten Expertinnen sowie Experten des Branchenarbeitskreises des UP KRITIS und schließlich von der Deutschen Krankenhausgesellschaft (DKG) vorgelegt.

Der B3S bietet wichtige Rahmenbedingungen, unter denen die Cyber-Sicherheit im Gesundheitswesen weiter erhöht werden kann. Er steht auch den vielen kleineren Kliniken, die nicht als KRITIS-Betreiber reguliert sind, zur Verfügung. Das kostenfreie Produkt gibt es zum Download auf den Webseiten der DKG. Die darin formulierten branchenspezifischen Empfehlungen sollten als Maßstab für die Umsetzung angemessener IT-Sicherheitsmaßnahmen dienen.

IT-Sicherheit: kein Kostenblock, sondern notwendige Investition in die Funktionsfähigkeit der medizinischen Versorgung

Die Digitalisierung im Gesundheitswesen eröffnet große Chancen für eine bessere Versorgung der Patientinnen und Patienten in der stationären medizinischen Versorgung. Informationssicherheit sollte dabei von Anfang an mitgedacht werden. Eine ganzheitliche und systematische Herangehensweise, die sich konsequent an der kritischen Dienstleistung orientiert, kann bei gleichzeitiger Steigerung des Sicherheitsniveaus mittel- und langfristig viel Aufwand sparen und darf nicht als bloßer Kostenfaktor abgetan werden.

Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI): „Um die Informationssicherheit auch weiterhin wirksam zu steigern, lohnt sich ein ganzheitlicher Ansatz.“



Was ist für den Start eines ISMS-Projekts im Krankenhaus wichtig?

ISMS-Aufbau für KRITIS-Krankenhäuser

Seit der Verabschiedung der NIS-Richtlinie müssen Krankenhäuser, die als Betreiber kritischer Infrastrukturen (KRITIS) eingestuft werden, ein Informationssicherheits-Managementsystem (ISMS) aufbauen. Ein ISMS ist ein System von Vorgaben und Abläufen, das die Informationssicherheit in einer Organisation sowohl definiert und umsetzt als auch dauerhaft steuert, kontrolliert, aufrechterhält und fortlaufend verbessert.

Der Aufbau eines ISMS ist kein einmaliges Projekt, welches einmal umgesetzt und anschließend abgeschlossen ist. Ein ISMS muss laufend betrieben, aktualisiert und erweitert werden, da die Bedrohungen und Risiken sich ebenfalls ständig verändern. Beim initialen ISMS-Aufbauprojekt ist es zudem wichtig, sich nicht im Detail zu verlieren. Betreiber kritischer Infrastrukturen sollten das Projekt zuerst mit einem „Basis-Setup" starten und anschließend regelmäßig mit weiteren Inhalten ergänzen.

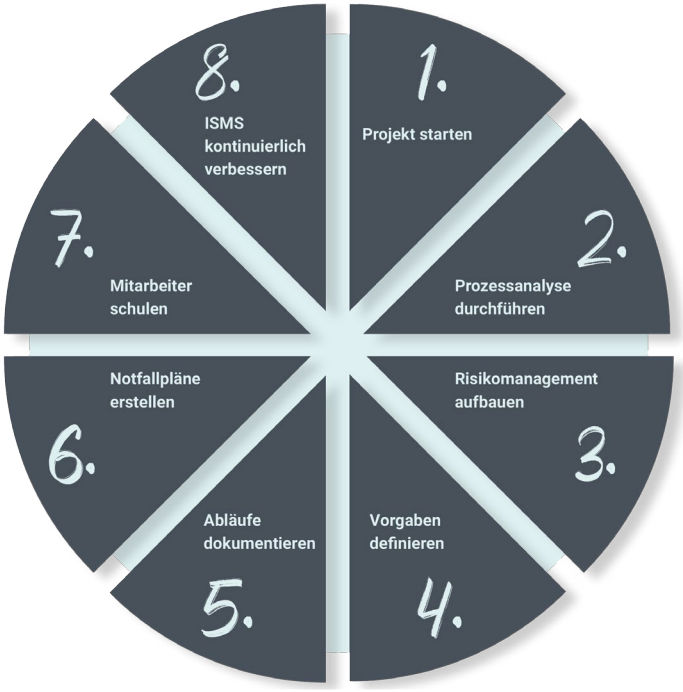
Welche Fachbereiche müssen beim ISMS-Projekt einbezogen werden?

Ein ISMS-Projekt ist kein reines IT-Thema und betrifft fast alle Fachbereiche eines Krankenhauses. Im Kernteam werden sich neben der IT auch Vertreter aus der Medizin- und Haustechnik sowie aus dem Datenschutz und dem Personalwesen wiederfinden. Für das Gelingen eines so umfangreichen Projektes ist es außerdem von großer Bedeutung, dass die Umsetzung vom obersten Management aktiv mitgetragen und als wichtiges Thema kommuniziert wird. Zusätzlich sollten die Verantwortlichen bei der Erstellung von Mitarbeitervorgaben an die frühzeitige Einbindung des Betriebsrates denken.

Welchen Umfang hat der ISMS-Aufbau für KRITIS-Krankenhäuser?

Im Krankenhausbereich orientiert sich der Geltungsbereich des ISMS an den Kernprozessen zur medizinischen Versorgung von Patienten. Üblicherweise sind dies die Aufnahme, Diagnose, Therapie, Pflege und Entlassung. Sämtliche Richtlinien, Prozessbeschreibungen und Dokumentationen sind auf diesen Umfang abzustimmen. Dies verdeutlicht nochmal, dass die IT-Abteilung allein ein solches Thema nicht vollumfänglich bewältigen kann.

Einen Überblick über den Aufbau eines Informationssicherheits-Managementsystems in einem Krankenhaus geben die folgenden acht Schritte:



1. Das Projekt starten

Zum Projektbeginn erfolgt ein gemeinsamer Kick-off-Termin mit Vertretern der relevanten Fachbereiche IT, Medizin- und Haustechnik, Datenschutz, Personalwesen sowie dem obersten Management. Bei diesem Termin wird der Projektauftrag, der Projektplan, das Kernteam und die jeweiligen Arbeitspakete für die einzelnen Beteiligen vorgestellt.

Praxistipp

Nur mit einem klaren Bekenntnis des obersten Managements zur Wichtigkeit eines derartigen Projektes ist ein erfolgreicher ISMS-Aufbau möglich.

2. Die Prozessanalyse durchführen

Im zweiten Schritt erfolgt die Analyse der Geschäftsprozesse und der medizinischen Kernprozesse. Dazu identifiziert das Kernteam alle internen und externen Beteiligten, die für die Sicherstellung der Kernprozesse – Aufnahme, Diagnose, Therapie, Pflege und Entlassung – notwendig sind. Danach erheben die Teammitglieder alle kritischen Prozesse und ermitteln für jeden als kritisch bewerteten Prozess, welche IT-Unterstützung zur dauerhaften Service-Erbringung notwendig ist. Hierbei unterscheidet das Team zwischen IT-Anwendungen aus Anwendersicht und IT-Komponenten aus IT-Infrastruktur-Sicht. Typische Krankenhaus-IT-Anwendungen sind beispielsweise KIS, LIS, RIS, PACS, DMS, OP-Planungssystem und Transportlogistik.

Praxistipp

Neben den üblichen Kernapplikationen im Krankenhaus sollten die Projektbeteiligten auch die IT-Systeme und Komponenten aus den Bereichen Medizintechnik, Versorgungstechnik (z. B. Wasser- und Energieversorgung), Kommunikationstechnik (z. B. Rufsysteme und Telefonie) und Informationstechnik (z. B. Domänen-Controller, IP-Datennetzwerke und Drucker) in ihren Prozessaufbau einbeziehen.

3. Das Risikomanagement aufbauen

Auf Basis der durchgeführten Geschäftsprozessanalyse erfolgt die Risikoanalyse der kritischen Prozesse im Krankenhaus. Die Projektteams erstellen dazu Risikokataloge, die sich aus den Anforderungen gängiger Normen – zum Beispiel ISO/IEC 27001 oder 27002 – sowie konkreter Serviceprozesse – zum Beispiel Absicherung der Übertragungswege vom und zum Service – ableiten lassen. Alle identifizierten Risiken werden in ein zentrales Informationssicherheits-Risikomanagementsystem überführt. Nach der Analyse und Bewertung werden anschließend geeignete Maßnahmen zur Risikobehandlung entwickelt.

Praxistipp

Beim initialen Aufbau eines Informationssicherheits-Risikomanagementsystems sind anfangs einfache Tabellen zur Dokumentation und Bewertung von Risiken ausreichend. Wichtiger ist vielmehr, dass das Kernteam eine nachvollziehbare Risikobewertungs-Systematik entwickelt und die jeweilige Bewertung, Auswirkung und Eintrittswahrscheinlichkeit in eigenen Worten begründet.

4. Die Vorgaben definieren

Jedes ISMS benötigt individuelle Leit- bzw. Richtlinien, die einerseits generelle Vorgaben wie Rollen, Verantwortlichkeiten und Management Commitment beinhalten und andererseits spezifische Regeln definieren – zum Beispiel die Entscheidungskompetenz eines Mitarbeiters oder einer Abteilung.

Praxistipp

Leit- bzw. Richtlinien sollten nicht „das Blaue vom Himmel" fordern, sondern der Wahrheit und Realität entsprechend formuliert sein. Das heißt, dass alle Vorgaben für die Mitarbeiter „einhaltbar" und nicht praxisfremd sind.

5. Alle Abläufe dokumentieren

Parallel zur Prozessanalyse erfolgt die Dokumentation der Prozesse und Abläufe. Meistens gibt es bereits „gelebte" Prozesse, die aber Großteils nicht oder nur unzureichend dokumentiert sind. Viele der zu dokumentierenden Prozesse betreffen dabei primär die IT, wie beispielsweise das Zugriffsmanagement, Backup- und Recovery-Prozesse oder das Schwachstellen-Management.

Praxistipp
Die Projektleiter sollten mit den jeweiligen Fachabteilungen Workshops in kleinen Gruppen durchführen und in einem ersten Schritt den IST-Stand dokumentieren. Dabei können sie eventuelle Abweichungen in das Informationssicherheits-Risikomanagement aufnehmen und diese dort analysieren und weiterbehandeln.

6. Die KRITIS-Notfallpläne erstellen

Das Vorhandensein von Notfallplänen ist in allen Krankenhäusern unerlässlich, denn die Patientenversorgung muss unter allen Umständen jederzeit gewährleistet werden. Daher ist nicht nur die Erstellung, sondern auch die Durchführung regelmäßiger Übungen Pflicht. Neben herkömmlichen Notfallszenarien – wie beispielsweise bei einem Brand – sollten auch IT-bezogene Notfallszenarien wie der Ausfall aller Rechenzentren betrachtet werden.

Praxistipp
Notfallpläne sollten an mehreren Stellen im Gebäude in ausgedruckter Form jederzeit griffbereit sein. Bei einem Komplettausfall der IT stehen diese Dokumente in digitaler Form nämlich nicht mehr zur Verfügung.

7. Alle Mitarbeiter ausbilden und regelmäßig schulen

Jeder Mitarbeiter muss über die wichtigsten Leit- und Richtlinien und deren Bedeutung unterrichtet und mithilfe laufender Schulungsmaßnahmen auf dem neuesten Stand gehalten werden. Mit einem praxistauglichen Schulungskonzept wird ein durchgängig hohes Sicherheitsniveau im Krankenhaus erreicht und dauerhaft sichergestellt.

Praxistipp
Aufgrund der großen Mitarbeiteranzahl im Gesundheitswesen hat sich eLearning als praxistaugliches Mittel etabliert. Mitarbeiter können selbst entscheiden, wann und wo sie eine Schulung absolvieren und werden nicht aus der Arbeit „herausgerissen". Zudem liefern eLearning-Systeme einen schnellen Nachweis über die Teilnahme und den Schulungsfortschritt. Führungskräfte können zusätzlich durch Workshops geschult werden, damit sie das Know-how in die jeweiligen Fachbereiche weitertragen können.

8. Das ISMS kontinuierlich verbessern

Nach erfolgter Einführung eines ISMS muss dieses „gelebt" und kontinuierlich verbessert bzw. erweitert werden. Dafür sollte das Kernteam messbare Kennzahlen definieren und mithilfe von Audits den aktuellen Stand überwachen. Durch die Auswertung der Kennzahlen und Audits lässt sich das ISMS anschließend steuern und kontinuierlich verbessern. Zudem sollte das Management als Betreiber der kritischen Infrastruktur aktiv in die Verbesserung des ISMS eingebunden werden. Am besten eignen sich dazu regelmäßige Management-Termine (z. B. quartalsweise) sowie ein jährlicher Management Review, also ein IST-Status mit den Ergebnissen aller Audits und den Kennzahlen sowie Verbesserungsvorschlägen.

Praxistipp
Versuchen Sie Kennzahlen messbar zu machen und grafisch darzustellen. Aussagekräftige Visualisierungen stellen eine optimale Entscheidungsgrundlage für das Management dar.

Michael Punz, CISO und Geschäftsbereichsleiter
Datenschutz & Informationssicherheit
+43 7242 2155-6325 | michael.punz@x-tention.at

KRITIS – Erfahrungen und Erfolge

Mit dem IT-Sicherheitsgesetz sollte die Basis für eine sichere Informationsverarbeitung und Kommunikation bundesweit geschaffen werden – vor allem in kritischen Bereichen, die das Allgemeinwohl betreffen, wie etwa der Gesundheitssektor. Allerdings zeigt die Erfahrung, dass weitere Anpassungen und Aktivitäten notwendig sind. Darauf sollten sich Betreiber von medizinischen Einrichtungen und Unternehmen der Gesundheitsbranche einstellen.

KRITIS ist nicht überall

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Betreiber Kritischer Infrastrukturen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

In der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) werden Kriterien angeführt, wann eine Organisation als Kritische Infrastruktur anzusehen ist. Dabei ist laut aktueller Regelung nur ein Bruchteil der deutschen Krankenhäuser und Unternehmen in der Gesundheitsbranche als Kritische Infrastruktur zu bezeichnen und mit entsprechenden Verpflichtungen beaufschlagt.

Da die Auflagen für Kritische Infrastrukturen einen mitunter gehörigen Einsatz von Geld, Personal und Zeit erfordern, legte der Gesetzgeber mit der Erstauflage der Kritisverordnung die Schwellenwerte so fest, um kleinere und mittlere Organisationen mit eher niedrigen IT-/Sicherheits-Budgets von den Verpflichtungen freizustellen – in der Annahme eines geringeren Risikos für die Allgemeinheit.

Es besteht weiterhin Anpassungsbedarf...

Allerdings hat sich gezeigt, dass auch Organisationen ohne KRITIS-Status angegriffen werden. Sie sind sogar besonders gefährdet, weil sie mangels Verpflichtung eher Schwächen in der Cybersicherheitsvorsorge aufweisen und ein Angriff umso erfolgversprechender ist. Von Cyberkriminellen werden sie als Einstiegspunkt oder Zwischenstation auf dem Weg zum eigentlichen Ziel bevorzugt und stehen dabei voll in der Haftung. Durch eine Anpassung der KRITIS-Schwellenwerte sollen absehbar weitere Einrichtungen zu Sicherheitsmaßnahmen verpflichtet werden, um die Abwehrlinie gegen Angreifer zu verbessern.

Die Gesundheitsbranche bewegt sich in einem hochdynamischen Umfeld, das eine ständige Neubewertung von Sicherheitsbedarf, Risiken und Schutzmaßnahmen erfordert. Neben technologischen und organisatorischen Neuerungen bzw. Änderungen sorgt auch der Gesetzgeber für zusätzliche oder gar verschärfte Anforderungen, etwa durch das E-Health-Gesetz oder das geplante IT-Sicherheitsgesetz (IT-SiG) 2.0.

Änderungsbedarf entsteht beispielsweise durch folgende Aspekte:

- Zunehmende Abhängigkeit von IT, Medizintechnik und Infrastrukturen
- Einsatz neuer Technologien
  (z.B. Mobile Computing, Digitalisierung, Archivierung, Künstliche Intelligenz)
- Nutzung neuer IT-Plattformen und Applikationen
  (z.B. Cloud Computing, Web-Anwendungen)
- Zusammenwachsen von Infrastrukturen
  (IT, Medizintechnik, OT, GLT - insbesondere auf Basis von TCP/IP)
- Veränderte oder neue Modelle der Zusammenarbeit
  (z.B. Telemedizin, Telemetrie, Datenaustausch)
- Fortschreitende und komplexere Einbindung von Lieferanten und Dienstleistungspartnern
- Wachsende Datenvolumina (z.B. PACS, RIS), gestiegene Echtzeit- und Synchronisationsanforderungen
- Veränderte oder neue Zugangs-, Authentifizierungs- und Berechtigungsteuerung
- Anspruchsvolle System-Migrationen
  (z.B. auf Betriebssystem- und Anwendungs-Ebene)
- Veränderte oder neue gesetzliche Anforderungen
  (z.B. E-Health-Gesetz, DSGVO)
- Erweiterte Compliance-Anforderungen (z.B. durch Geschäftspartner)
- Veränderte, fortgeschrittene Angriffsvektoren
- Angriffe unabhängig von der Organisationsgröße

Auf jeden Fall kritisch aus Sicht der Organisationsleitung sind Ereignisse, die die Funktionsfähigkeit einer Organisation beeinträchtigen, deren Ruf schädigen und letztlich die Finanzierungs-, schlimmstenfalls sogar die Existenzgrundlage gefährden können.

... und Handlungsbedarf

Diese Ereignisse zu erkennen, zu steuern und erfolgreich zu behandeln, setzt ein wirksames Informationssicherheits-Management voraus. Schon aus Verantwortungsbewusstsein gegenüber der eigenen Organisation und den von ihr versorgten Patienten sollten Krankenhäuser unabhängig von ihrer KRITIS-Einstufung ein risikobasiertes Informationssicherheits-Managementsystem (ISMS) in angemessener Weise betreiben. Eine zusätzliche Zertifizierung gemäß ISO 27001 oder B3S hilft beim Nachweis, aktiv zur Absicherung der Einrichtung und damit zum Patientenwohl beigetragen zu haben.

Dabei sollten sich medizinische Einrichtungen besonders folgenden Themen widmen, auch weil sich hier bei Audits regelmäßig Defizite offenbaren:

- Umfassendes und übergreifendes Asset-Management: IT, Medizintechnik/Modalitäten, weitere Systeme samt Verantwortlichkeiten und Schutzbedarf-Feststellung/Kategorisierung
- Konsequentes Risiko-Management: Erkennung, Bewertung und Behandlung von Risiken als Schlüssel zur Wirtschaftlichkeit von Maßnahmen
- Aktives (Security) Incident Management mit Überwachung eingesetzter Komponenten (IT/TK, Medizintechnik, OT/GLT, Infrastrukturen)
- Strukturiertes Change-Management (vor allem zur Absicherung und Optimierung von Abläufen)
- Konsolidierung von Infrastrukturen zur Kostenoptimierung sowie zur effektiven und effizienten Steuerung auf Basis von Informationssicherheits-Anforderungen
- Gezielte Segmentierung von Infrastrukturen/Netzen und Absicherung durch Security Gateways
- Schaffung angemessener Redundanzen (Systeme, Infrastruktur – etwa Lichtruf, WLAN intern/Patienten/extern)
- Notfall-Management und Business Continuity Management, einschließlich Notfallübungen
- Lieferanten-Management: Vertragsgestaltung, insbesondere OLA/SLA im Hinblick auf Anforderungen der Informationssicherheit/KRITIS; Lieferanten-Audit usw.
- Beschaffung: (Standard-)Anforderungen im Hinblick auf Informationssicherheit für Produkte und Dienstleistungen definieren, vertraglich fixieren und Einhaltung überprüfen
- Dokumentations-Management: Informationen hilfreich und rechtskonform ablegen/archivieren
- Awareness-Management: regelmäßige und dokumentierte Maßnahmen für Personal, Geschäftspartner usw.

Zur Abschätzung insbesondere von zukünftig erforderlichen Maßnahmen lohnt ein Blick in den Entwurf des IT-SiG 2.0. Dort ist beispielsweise ein verpflichtender Einsatz von Systemen zur Anomalieerkennung beim Datenverkehr (etwa infolge von Cyberangriffen, Ausspähversuchen usw.) vorgesehen.

Auch Hersteller und Lieferanten sollten sich den gestiegenen Erwartungen stellen und Informationssicherheits-Anforderungen aktiv und konsequent bei der Gestaltung von Produkten und Dienstleistungen berücksichtigen. Im Entwurf des IT-SiG 2.0 ist beispielsweise als Voraussetzung für den Betrieb von Produkten in Kritischen Infrastrukturen die Vergabe eines Sicherheits-Prüfsiegels vorgesehen, für das entsprechende Nachweise vorzulegen sind.

KRITIS ist doch überall

KRITIS ist doch überall – so sollte es zumindest von Betreibern medizinischer Einrichtungen und Unternehmen in der Gesundheitsbranche gesehen werden.

Der Entwurf zum IT-SiG 2.0 sieht bei Nichterfüllung der KRITIS-Anforderungen Sanktionen gleichlautend zur DSGVO vor. Damit würde sich der Blick auf notwendige Investitionen verändern und die Bewertung der Wirtschaftlichkeit von Maßnahmen auf ein neues Fundament stellen. Für Einrichtungen, die trotz angedachter Schwellenwerte (noch) nicht zu einer Kritischen Infrastruktur werden, drohten bei Nichterfüllung zwar keine Sanktionen durch die Aufsichtsbehörde, möglicherweise aber auf zivil- oder strafrechtlichem Wege, wenn sie im Falle einer Schädigung von Patienten den Nachweis schuldig bleiben, dem aktuellen Stand der Technik entsprochen zu haben.

Um schnell und ohne unnötigen Aufwand zum Ziel zu kommen, kann eine fachkompetente und zertifizierte externe Unterstützung dabei behilflich sein, rasch ein wirksames ISMS im Einklang mit den KRITIS-Anforderungen zu etablieren, dieses wirtschaftlich zu betreiben, dabei von den Erfahrungen aus anderen Projekten zu profitieren und zahlreiche Mehrwerte zu nutzen. Des Weiteren kann ein externer Partner dabei unterstützen, das erforderliche Sicherheits-Niveau zu erreichen, zu halten und zu optimieren.

Sascha M. Zaczyk
Manager Informationssicherheit & Premium Consultant, International Certified Lead Auditor ISO 27001, zertifizierter Lead Auditor EN 50600, zertifizierter (Agile) ITIL-Experte & Datenschutzbeauftragter, Professional Scrum Master;
Kontakt: IT-Gutachter@gmx.de

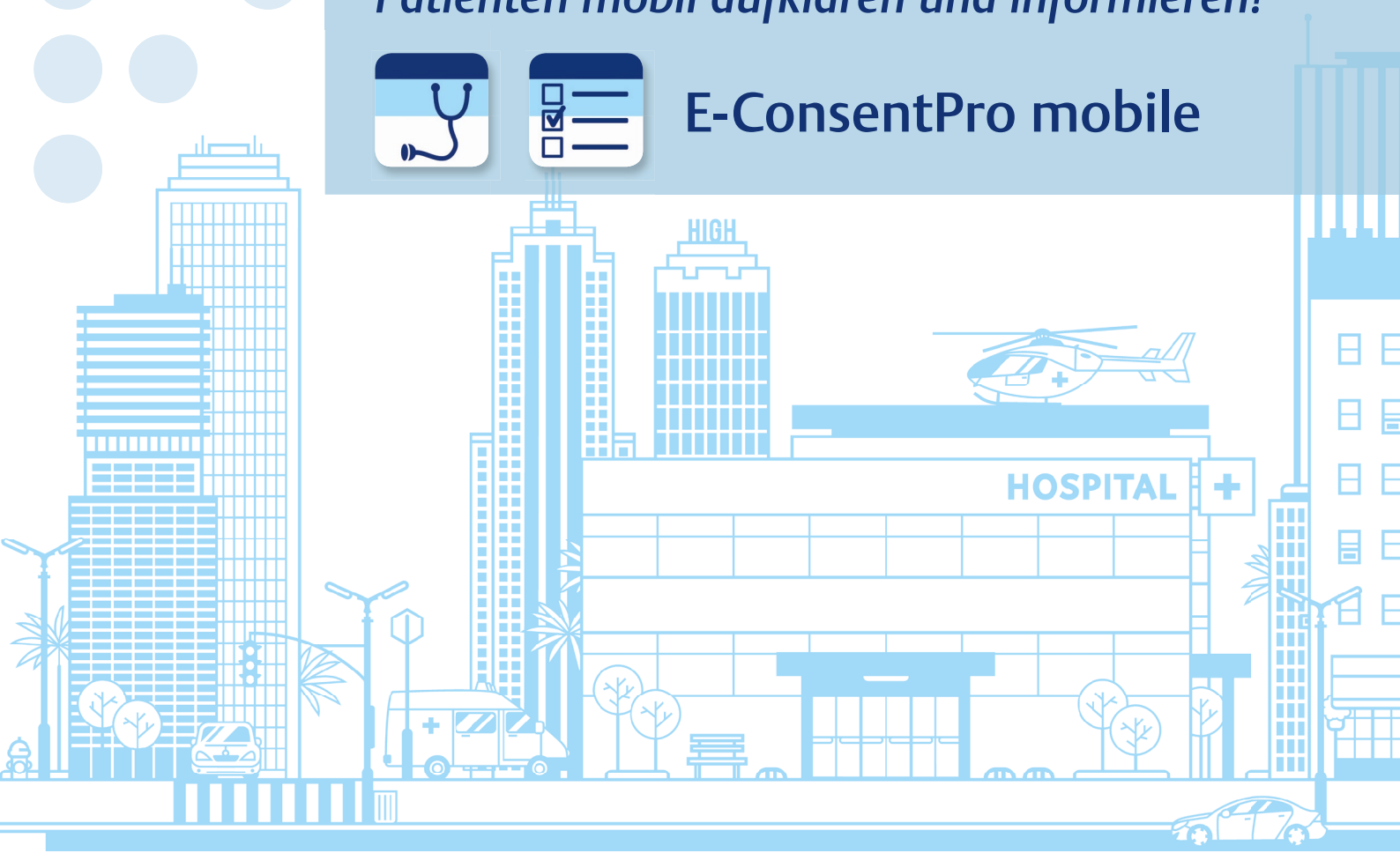
Patientenaufklärungsbögen und eigene Dokumente digital bearbeiten, unterschreiben und sicher archivieren

Eigene Dokumente komplett digital!

E-DocumentPro

Patienten mobil aufklären und informieren!

E-ConsentPro mobile



www.thieme-compliance.de

Thieme Compliance

KRITIS-Umsetzung im Klinikum Frankfurt Höchst – *mit ganzheitlicher Lösungsorientierung zur erhöhten Informationssicherheit*

Das Klinikum Frankfurt Höchst gehört mit mehr als 37.000 stationären Patienten in die Gruppe der „kritischen Infrastrukturen“ KRITIS. Schnell war dem Krankenhaus-Management klar, dass mit dem KRITIS-Status zügig die vollständige Umsetzung des IT-Sicherheitsgesetzes beginnen muss. Die inhaltliche Auseinandersetzung mit den geforderten Themen machte deutlich, dass für den Projekterfolg externe Unterstützung notwendig sein würde.

Aus dieser Situation heraus ist eine intensive Zusammenarbeit mit dem Darmstädter IT-Beratungsunternehmen Adiccon GmbH entstanden, mit dessen praxisorientierter Unterstützung das Klinikum die KRITIS-Prüfung zum 30.06.2019 erfolgreich absolvierte.

Ganzheitlicher Ansatz

Die Erfahrungen für alle Projektbeteiligten des Klinikums sind vielfältig. Dr. Thomas Seehaus, Abteilungsleiter EDV/Medizininformatik erinnert sich: „Am Anfang des KRITIS-Projektes war es für viele in unserem Haus schwer nachzuvollziehen, dass es sich um eine unternehmensweite Aufgabenstellung handeln muss.“

Man traf die Entscheidung, sich am von der DKG getragenen und im Entwurf vorliegenden branchenspezifischen Standard (B3S) zu orientieren. Die Projektarbeit zeigte, dass eine Reihe von Themen bekannt war, nun aber Maßnahmen zur Lösung präzise umgesetzt werden mussten. Dazu gehörten u.a. Zuständigkeiten festlegen, Erstellen der Informationssicherheitsleitlinie und des Risikomanagement-Konzepts – zusammen mit der Definition der kritischen Prozesse im Klinikum.

Risikobetrachtung als Herausforderung

Weitgehend neu waren die Themen rund um das Risikomanagement von IT-Lösungen und –Infrastrukturen. „Die Menge von gelisteten Risikoobjekten war schon beachtlich.

Die Beurteilung und Einschätzung durch die Verantwortlichen gestaltete sich schwierig. Alle mussten sich erst einmal mit der gedanklichen Logik zu Recht finden", so Thomas Seehaus. Sukzessive wurde der strukturelle Rahmen eingeführt – das Information Security Management System (ISMS) nahm Formen an.

Um die gesetzlichen Anforderungen fristgerecht umzusetzen, bestand ein wichtiger Erfolgsfaktor darin, die Funktion des Informationssicherheitsbeauftragten extern mit einem Fachmann der Adiccon zu besetzen. Als zentraler Ansprechpartner begleitet der ISB auch nach der Prüfung im Juni 2019 die weiteren Umsetzungsmaßnahmen, die das gesamte Sicherheitsniveau des Klinikums im Hinblick auf die Informationssicherheit kontinuierlich erhöhen. In Zeiten immer perfider werdender Cyber-Attacken geht es konkret um die organisationsweite Optimierung der Sicherheit. Dr. Seehaus stellt fest: „Ein konkreter Erfolg des KRITIS-Projektes ist die strukturierte und stetige Verbesserung unseres Sicherheitsstandards gemeinsam mit dem ISB. Dazu gehörte für uns ganz klar das Aufrüsten unserer Sicherheitsmechanismen sowie die Schulung unserer Mitarbeiter gegenüber aktuellen Cyber-Attacken."

Digitalisierung und Informationssicherheit

Zudem erfordert die umfassende Digitalisierung der Prozesse, sich intensiv mit Themen wie dem IT-Notfallmanagement auseinanderzusetzen. Durch eine intensive Begutachtung der Risikoobjekte und einer aktiven Risikobewertung gewinnen die entsprechenden Organisationseinheiten und das Krankenhausmanagement dazu einen guten Überblick, der in dieser Feinheit vorher nicht vorhanden war. Das Risikomanagement wird damit kontrollierbar und kann jederzeit nachvollzogen werden. Mehr noch: Es kann mehr und mehr dazu übergegangen werden, präventive Schutzmaßnahmen und -vorkehrungen zu treffen, wie beispielsweise bedarfsgerechte Awareness-Maßnahmen für die Mitarbeiter mit zeitgemäßen Technologien anhand von E-Learning Kursen.

Transparenz durch Tool-Einsatz

Im Laufe der Risikobetrachtung wurde deutlich, dass das erfasste Datenvolumen stetig steigt. Eine übersichtliche, dem Management-Blick gerecht werdende Darstellung der Ergebnisse ist mit herkömmlichen Mitteln kaum oder gar nicht zu erreichen. Dr. Seehaus kommentiert: „Es ist erstaunlich, wie viele Daten generiert und wie viele Risikoobjekte erfasst werden, die dann auch beurteilt werden müssen – und das unter Berücksichtigung des B3S. Da waren wir sehr froh, dass unser Beratungspartner mit seiner Kombination aus Krankenhaus-Know-how und Informations-Sicherheits-Expertise uns obendrein noch ein eigenentwickeltes Risikomanagement-Tool anbieten konnte. Mit AdiRisk haben wir begonnen, unser IT-Risikomanagement strukturiert und mit hoher Transparenz abzubilden."

KRITIS bedeutet Innovation

Ein weiterer wichtiger Aspekt resultiert als Erfahrung und als Erfolg aus dem KRITIS-Projekt: Die genaue Begutachtung aller eingesetzten Lösungen führt automatisch zu einer umfassenden Bestandsaufnahme. Damit entstehen auch Ideen, wie moderne Technologien für den Einsatz im klinischen Bereich sinnvoll sind, beispielsweise für ein mobiles Arbeiten. Informationssicherheit löst deshalb nicht nur Restriktionen aus, sondern schafft auch Impulse für innovative Maßnahmen, z.B. die interne Kommunikation für Mediziner zu verbessern.

Was der IT-Leiter meint

KRITIS-Erfahrungen

Beim Thema KRITIS und der Umsetzung geht Thorsten Schütz auf drei typische Fragestellungen ein: Wie ist es gelaufen? Wer soll das bezahlen? Wer kümmert sich um die Prozesse? Aus der subjektiven Sicht eines IT-Leiters stellt der Autor offensiv Erfahrungen und Thesen vor mit engem Blickkontakt zur Realität in Krankenhäusern.

***Thorsten Schütz** ist Leiter IT und Betriebsorganisation, Klinikum Itzehoe, und Vorstand im KH-IT.*

Erfahrungen aus dem Prüfnachweis

Rund 120 Krankenhäuser in Deutschland mussten im vergangenen Jahr gemäß KRITIS-Verordnung erstmalig den §8a-Prüfnachweis gemäß BSI-Gesetz (Bundesamt für Sicherheit in der Informationstechnik) erbringen, da sie die Grenze von mehr als 30.000 stationären Fällen pro Jahr überschritten hatten. Die betroffenen Krankenhäuser, genauso wie Prüfteams und BSI, betraten damit weitgehend Neuland und so wundert es nicht, dass einige Anlaufschwierigkeiten zu überwinden waren.

Vielfach wurde zum Beispiel das Finden eines geeigneten Prüfteams völlig unterschätzt. Zwar wurden frühzeitig seitens des BSI geeignete Kurse für Prüfer zur Erlangung der §8a Prüfverfahrenskompetenz angeboten, doch zusätzlich geforderte Befähigungen der Prüfer wie Audit-Kompetenz, IT-Sicherheitskompetenz und insbesondere die notwendige Branchenkompetenz stellten oftmals selbst größere Beraterfirmen überraschend vor Herausforderungen. In der Folge hatte so manches Krankenhaus unerwartet Probleme, vor Ablauf der Frist passende Prüfer zu finden. Eine zentrale Liste prüfender Instanzen, wie von vielen Krankenhäusern regelmäßig nachfragt, sucht man bislang noch vergebens.

War diese Herausforderung gelöst, galt es im Anschluss, den Prüfnachweis in geeigneter Form zu erstellen. Mangels Vorerfahrungen, auf die hierbei zurückgegriffen werden konnte, kann davon ausgegangen werden, dass die abgegebenen Prüfnachweise bei diesem ersten Durchlauf von durchaus sehr unterschiedlicher Qualität gewesen sind. Für die nächste Runde im Sommer 2021 könnte das strukturierter werden. Basierend auf den jetzigen Ergebnissen, die sich noch in der Auswertung befinden, werden voraussichtlich konkrete Vorgaben entwickelt, was die Vergleichbarkeit der abgefragten Daten vereinfachen würde. Ohnehin wird die Datenbasis dann vermutlich größer sein, zahlreiche Experten erwarten in den kommenden Monaten eine Absenkung der bisher gültigen Fallzahlschwelle und damit eine Ausweitung der Anzahl derjenigen Krankenhäuser, die unter das BSI-Gesetz fallen.

IT-Sicherheit und finanzielle Förderung

Mit Absenkung der Fallzahlschwelle rückt dann schnell das Thema der Finanzierung erneut in den Blickpunkt. Orientiert man sich allein am zugrundeliegenden IT-Sicherheitsgesetz, dürften für Betreiber einer kritischen Infrastruktur wie z. B. Krankenhäuser, durch die Einhaltung der BSI-Vorgaben keine nennenswerten Mehrkosten durch Erfüllungsaufwände entstehen. Es kann nämlich davon ausgegangen werden, dass KRITIS Betreiber ohnehin ein Eigeninteresse, das sogenannte Mindestsicherheitsniveau einzuhalten, besitzen. Vor dem Hintergrund der zahlreichen Ransomware-Attacken auf Krankenhäuser in den letzten Jahren ist diese Argumentation durchaus naheliegend. Auf der anderen Seite zeigt die Realität, in Krankenhäusern besteht durchaus vielfach Verbesserungspotential in Sicherheitsfragen. Nicht ohne Grund wurden explizit finanzielle Fördermöglichkeiten für KRITIS-Häuser z. B. über das Pflegepersonal-Stärkungsgesetz in Aussicht gestellt. Die Vergabe dieser Fördermittel fällt jedoch in die Hoheit der Länder, und im Ergebnis verfahren die Bundesländer hier höchst unterschiedlich. In vielen Bundesländern ist keinerlei Förderung vorgesehen, andere Länder unterstützen neben den KRITIS-Häusern zusätzlich auch Krankenhäuser, die nicht unter das IT-Sicherheitsgesetz fallen. Viele Betroffene wünschen sich hier klarere Vorgaben, zumal wenn mit Ausweitung der betroffenen Häuser zukünftig weitere kleine, weniger finanzstarke Kliniken mit unter das IT-Sicherheitsgesetz fallen sollten und damit die Fördernachfrage steigen wird. Dank unabhängiger Erhebungen zum diesem Thema, beispielsweise veranlasst durch die Deutsche Krankenhausgesellschaft (DKG), gibt es durchaus valide Zahlen zum Bedarf, auf denen man hier aufbauen könnte.

Prozesse im Mittelpunkt

Eine unerwartete Herausforderung im Zusammenhang mit dem IT-Sicherheitsgesetz und den daraus abgeleiteten Prüfungen ergibt sich an einer weiteren Stelle.

Die Schaffung von IT-Sicherheit beginnt oft mit der fachgerechten Umsetzung zahlreicher technischer Maßnahmen. Für die geeignete Implementation eines Informationssicherheitsmanagementsystems (ISMS), für die Priorisierung von Maßnahmen oder für das Aufsetzen von Ausfallkonzepten und Notfallplänen sind zuallererst jedoch das Verständnis und die Analyse der zugrundeliegenden Prozesse unabdinglich. Als Orientierung gibt der Branchenspezifische Sicherheitsstandard (B3S) mit den zentralen Säulen Aufnahme, Diagnose, Therapie, Pflege und Entlassung Kategorien vor, nach denen sich Kern- und Unterstützungsprozesse, fachrichtungsbezogen zuordnen und beschreiben lassen. Genau hier entzündet sich in vielen Krankenhäusern die Frage: Wer ist für die Beschreibung und Analyse dieser Prozesse zuständig?

Der IT-Sicherheitsbeauftragte, in der hierarchischen Stellung vergleichbar mit dem Datenschutzbeauftragten, ist vielerorts bereits installiert, insbesondere in den KRITIS-Häusern. Er sieht seine Aufgabe jedoch meist darin, fertige Prozessbeschreibungen auf IT-Sicherheit zu prüfen und weniger darin, diese selbst zu erstellen. Die Anwender wie z. B. Ärzte und Pflegeverantwortliche kennen ihre täglichen Prozesse und die damit verbundenen Risiken und Gefährdungen natürlich am besten. Ihnen fehlt es jedoch oftmals an der Methodik sowie den geeigneten Werkzeugen und im Klinikalltag nicht zuletzt an der Zeit, sich dieses Themas anzunehmen. Ein eigens benannter Prozessbeauftragter, der diese Lücke füllt, fehlt bislang in den Krankenhäusern. Die Vergabe an externe Berater sollte aufgrund der damit verbundenen Kosten und der Auslagerung von elementarem, hauseigenen Prozesswissen nur die letzte Option bleiben.

Bleibt noch die IT im Krankenhaus, nach eigener Einschätzung ebenfalls oft bis an die Grenzen ausgelastet. Trotzdem sollten gerade die IT-Verantwortlichen überlegen, ob nicht das Prozesswissen, welches in ihrer Abteilung aufgrund der applikationsübergreifenden Sichtweise vielfach in überdurchschnittlicher Ausprägung vorhanden ist, genutzt werden kann, dieses in Richtung Prozessvisualisierung und Prozessanalyse weiter auszubauen. Ohnehin wird es niemals den einen geben, der alle Prozesse in einem Krankenhaus vollständig kennt. Stattdessen ist eine Abteilung gefragt, die erhebend und moderierend das Prozesswissen zahlreicher Beteiligter zusammenträgt und in eine sinnvoll aufbereitete Form überführt. Darauf aufbauend lässt sich dann zum einen die IT-Sicherheit stetig verbessern, zum anderen können daraus weitere Wertschöpfungspotentiale und Effizienzgewinne abgeleitet werden. So kann die Beschäftigung mit IT-Sicherheit in vielfacher Hinsicht zu einem Gewinn für das gesamte Haus werden.

Thorsten Schütz, Leiter IT und Betriebsorganisation, Klinikum Itzehoe, und Vorstand im Bundesverband der Krankenhaus IT-Leiterinnen/Leiter e.V. (KH-IT): „So kann die Beschäftigung mit IT-Sicherheit in vielfacher Hinsicht zu einem Gewinn für das gesamte Haus werden."

Informationssicherheit gehört automatisch in alle Krankenhausprozesse

An erster Stelle bei KRITIS steht die Mitarbeiter-Awarenes

Noch ist die Informationssicherheit kein fester Bestandteil der Krankenhauswelt. Mehr als 30.000 vollstationäre Fälle pro Jahr ist jedoch jene kritische Marke, bei der Krankenhäuser besondere IT-Sicherheitsstandards nachweisen müssen: KRITIS. Der systematische Blick darauf sollte für Krankenhäuser zur Alltäglichkeit werden . Dies gilt für Instrumente, Maßnahmen - und besonders Mitarbeiter.
Jens Schulze, Dezernent / CIO, Universitätsklinikum Frankfurt, skizziert Perspektiven.

Welche Erfahrungen haben IT-Verantwortliche mit KRITIS bisher gemacht?

Aus Gesprächen mit anderen Einrichtungen muss man feststellen, dass jeder Betreiber einer kritischen Infrastruktur im Krankenhausumfeld zum Thema KRITIS aus dem Audit zur Nachweiserbringung einen anderen Weg geht. Jeder Betreiber hat trotz gleicher Aufgaben- und Problemstellungen einen anderen Fokus und eine andere Zielsetzung, so dass jeder dieser Betreiber gerade für sich das Rad neu erfindet. Das sieht man auch an den aktuellen Diskussionen bei den Betreibern kritischer Infrastruktur im Krankenhausumfeld zu den verschiedenen Prüfgrundlagen. Die einen hatten beispielsweise zur Nachweiserbringung den Branchenstandard B3S als Prüfgrundlage und wollen zukünftig die ISO/IEC 27001 dafür als Grundlage nutzen und umgekehrt. Die Begründungen für den Wechsel der Prüfgrundlage sind oft nicht schlüssig und valide, belasten nur knappe Ressourcen und kosten viel Zeit. Aufgrund der unterschiedlichen Prüfgrundlagen zur Nachweiserbringung sind auch die Ergebnisse zu ein und demselben Thema aus den Nachweiserbringungen komplett verschieden. Vergleichbarkeit zur Einhaltung „Stand der Technik" so nicht möglich.

Wo drückt der KRITIS-Schuh in Kliniken besonders?

Egal ob in Krankenhäusern oder anderen Branchen, die meisten erfolgreichen Zwischenfälle hatten überwiegend die Schwachstelle „Mensch" als Ursache. An erster Stelle muss in jedem Krankenhaus und Unternehmen die regelmäßige Mitarbeiter-Awareness zur Informationssicherheit stehen. Sämtliche bisher vorhandene Schwachstellen stehen mit dem menschlichen Handeln in Verbindung. Sei es, dass zum Beispiel die menschliche Neugierde ausgenutzt wird oder die menschliche Bequemlichkeit eine Ursache für technische und organisatorische „Schlupflöcher" ist.
Auch ist in den Krankenhäusern aktuell zu erkennen, dass die Informationssicherheit noch kein fester Bestandteil der Krankenhauswelt ist. Bis dato liegt in vielen Krankenhäusern, die zur kritischen Infrastruktur gehören, der Fokus zur Informationssicherheit primär auf den Nachweiserbringungen. Die Aktivitäten zur Informationssicherheit im Krankenhaus haben bisher wenige Verknüpfungen zum täglichen Krankenhausbetrieb, sondern werden rein an die bevorstehende Nachweiserbringung oder an bevorstehende Audits geknüpft.

Jens Schulze, Dezernent / CIO, Universitätsklinikum Frankfurt: „Egal ob in Krankenhäusern oder anderen Branchen, die meisten erfolgreichen Zwischenfälle hatten überwiegend die Schwachstelle „Mensch" als Ursache."

Was ist vor allem von den Krankenhäusern künftig zu tun?

Informationssicherheit muss in den Krankenhäusern zukünftig zur unbewussten Kompetenz der Krankenhäuser dazugehören, und das wird nur durch regelmäßige Awareness-Maßnahmen der Mitarbeiter im Unternehmen erreicht. Informationssicherheit muss in allen Krankenhausprozessen automatisch mit Berücksichtigung finden. Aufgrund der Überschneidungen zu den Themen: Datenschutz, Qualitätsmanagement/ Patientensicherheit, usw. mit der Informationssicherheit, sollten alle diese Bereiche im Krankenhaus eng verknüpft miteinander zusammenarbeiten und die Synergien gemeinsam nutzen, weil sonst die Gefahr besteht, dass thematisch gleiche Parallelstrukturen entstehen, die wiederum kostbare Ressourcen im Krankenhaus binden.

KRITIS: Herausforderung für Krankenhäuser ist die Umsetzung

Kampf um Sicherheit, Ordnungsmäßigkeit, Wirtschaftlichkeit

Der KRITIS-Schuh drückt nicht wenige Kliniken. Die gute Nachricht: Durch Prüfnachweise lassen sich Verbesserungen ableiten. Allerdings besteht die Herausforderung für Krankenhäuser in der Umsetzung. Was von den Krankenhäusern vor allem bei KRITIS-Maßnahmen zu tun ist, skizziert Lars Forchheim. Er ist Leiter des Branchenarbeitskreises Medizinische Versorgung und CIO der ANregiomed.

Welche positiven Erfahrungen haben IT-Verantwortliche mit KRITIS bisher gemacht?

Lars Forchheim: Bei dem Thema KRITIS habe ich die Erfahrung gemacht, dass Agieren besser ist als Reagieren. Es geht um die Informationssicherheit innerhalb des Unternehmens. Im Kern handelt es sich um die Risikominimierung „eines Ausfalls" der kritischen Dienstleistung. Damit handelt es sich um die Absicherung der Patientenversorgung. Der Branchenarbeitskreis (BAK) Medizinische Versorgung ist dabei ein klarer Gestalter und bringt durch seine Experten entsprechende Handlungsempfehlungen heraus bzw. gibt den nötigen Input für z.B. die Erstellung/Anpassung des B3S.

Die Erfahrungen entstehen bei diesem Thema durch Sicherheits-Angriffe und damit der Störung der kritischen Dienstleistung. Hierbei steht nicht die Ursache allein im Fokus, vielmehr steht das Lernen daraus im Vordergrund:

- *Was machen wir, wenn es passiert?*
- *Wie gehen wir vor?*
- *Wer muss informiert werden?*
- *Welche Maßnahmen leiten sich ab?*
- *Was lernen wir daraus?*

Der BAK dient dabei als Plattform, um Erfahrungen, Netzwerk und Hinweise zu erhalten.

In meiner Wahrnehmung ist gerade die Mitnahme aller Mitarbeiter eine Herausforderung. Die Informationssicherheit macht die Systeme besser, jedoch ändern sich dadurch auch Abläufe und Prozesse. Der „innere Schweinehund" der Mitarbeiter muss ausgetrieben werden. Hierzu müssen die Mitarbeiter eingebunden werden. Weiterhin muss man von positiven Erfahrungen berichten und Anreize schaffen.

Eine Wissenserweiterung bringt ein Penetrationstest innerhalb der Organisation. Dass es Lücken gibt, ist bekannt, jedoch wo und wie viele, bleibt meistens eher im Verborgenen. Weiterhin lassen sich damit den Mitarbeitern Beispiele besser darstellen.

Wo drückt der KRITIS-Schuh in Kliniken besonders?

Lars Forchheim: Ein Thema ist die Finanzierung. Es gibt seitens Bund entsprechende Strukturfonds. Jedes Bundesland hat dafür entsprechende Regelungen zum Abruf. Der Abruf erfolgt jedoch pro Bundesland unterschiedlich, und die Finanzierung ist zum Großteil auf Investitionen ausgelegt. Bei Informationssicherheit geht es aber vor allem um den Betrieb, also um die Wartung und die dazu nötigen Ressourcen.

Ein weiterer Fokus liegt auf dem Änderungsprozess. Mit der Einführung eines neuen Systems bzw. Prozesses ist es nicht getan. Diese Änderungen benötigen Zeit, und die Mitarbeiter müssen sich an die neuen Abläufe gewöhnen. Teilweise verlieren sie aus Sicht der Mitarbeiter entsprechende Flexibilität. Sie gewinnen aber an Sicherheit, und das muss kommuniziert werden.

Was ist von den Krankenhäusern vor allem bei technischen und organisatorischen KRITIS-Maßnahmen und damit verbundenen Problemen zu tun?

Lars Forchheim: Am 30.06.2019 war der erste Prüfnachweis von Häusern entsprechend des Schwellenwertes zu erfüllen. Aller zwei Jahre ist dieser zu erbringen. In dem Prüfnachweis geht es im Wesentlichen um eine Momentaufnahme und die Betrachtung von Risiken und somit deren Maßnahmen zur Reduzierung. Dieser Prozess bringt entsprechende Herausforderungen mit sich. Es beginnt bei der „Suche" nach einer

prüfenden Stelle und endet bei der Umsetzung der jeweiligen Maßnahme. Durch die „erste" Welle der Prüfnachweise lassen sich Verbesserungen ableiten. Hier sind die Vorgaben, z.B. B3S aber auch Prüfnachweisdokumente, zu verbessern. Der Branchenarbeitskreis legt gerade darauf seinen aktuellen Arbeitsschwerpunkt.

Die Herausforderungen für Krankenhäuser besteht besonders in den Umsetzungen der Maßnahmen. Die Umsetzung benötigt vor allem Zeit, und dies ist abhängig von den Ressourcen. Auf der einen Seite müssen die Abläufe angepasst werden. Auf der anderen Seite werden Personalressourcen und Budgets benötigt. Somit kämpfen die Krankenhäuser um die Reihenfolge der Sicherheit, der Ordnungsmäßigkeit und der Wirtschaftlichkeit. Dieser Kampf muss gemeinsam auf der Führungsebene zusammen mit den jeweiligen Beauftragten abgestimmt werden und die Ergebnisse allen Mitarbeitern transparent kommuniziert werden.

Lars Forchheim, KH-IT-Vorstand: „Die Herausforderungen für Krankenhäuser besteht besonders in den Umsetzungen der Maßnahmen." https://www.kh-it.de

Wachmacher für die Krankenhäuser

KRITIS – Befund und Prognose

KRITIS war und ist ein Wachmacher für die Krankenhäuser. Die Umsetzung der strengen Anforderungen führt derzeit zu einem spürbaren Bewusstseinswandel. Die Klinken betrachten nun ihre als kritisch eingestufte und elementare Dienstleistung durch ein Informationssicherheitsmanagementsystem (ISMS) und damit vollumfänglich anhand von Sicherheitsaspekten. ***Von Olaf Janßen ist Leiter Information Security Management für die Geschäftsbereiche Public Sector und Healthcare Management von Sopra Steria.***

Die Pflicht zur Umsetzung von KRITIS-Anforderungen schärft vor allem das Bewusstsein des zuständigen Personals. Die Anwendung des Branchenstandards B3S vereinheitlicht zudem die Abläufe und das Denken und ermöglicht den Austausch der KRITIS-relevanten Krankenhäuser untereinander.

Indem Krankenhäuser Prozesse von Anfang bis zum Ende durchdenken um im Anschluss ein ISMS implementieren, schafften sie die Voraussetzung, mit der zunehmenden Digitalisierung im Gesundheitswesen aus Sicht der Cybersicherheit Schritt zu halten.

IT- und Medizin-Notfallmanagement verzahnen

Knackpunkt einer ISMS-Implementierung ist in vielen Häusern die Einführung eines klinischen Kontinuitätsmanagements. Der in diesem Rahmen gültige branchenspezifische Sicherheitsstandard (B3S) zur stationären medizinischen Versorgung ist eindeutig und enthält dezidierte Anforderungen zum Notfallmanagement. Dazu gehört zum Beispiel die Verzahnung des IT-Notfallmanagements mit dem klinischen Notfallmanagement.

Festzustellen ist, dass Krankenhäuser zwar Vorkehrungen treffen, um mögliche Auswirkungen von Schadensszenarien zu reduzieren, aber diese nicht erproben. Zu groß ist die Sorge vor dem Schaden durch die Notfallübung. Aber auch hier gilt: Nur was Kliniken ausreichend eingeübt haben, können sie im realen Notfall abrufen.

Security Operation Center auch für Medizintechnik einführen

Kontinuitätsmanagement ist nicht nur bei Notfällen wichtig. Angriffsvektoren entwickeln sich ständig weiter. Die Leistungserbringer im Gesundheitswesen sind somit gefordert, sich nicht auf ihrem einmal eingeführten ISMS auszuruhen, sondern es ebenfalls laufend anzupassen. Die Prämisse sollte lauten: kontinuierlich Maßnahmen erarbeiten, die für das Krankenhaus geeignet, angemessen, verhältnismäßig und vor allem wirksam sind. Reifegradmodelle sind dafür ein geeignetes Hilfsmittel.

Darüber hinaus müssen Krankenhäuser ihre Infrastruktur kontinuierlich überwachen. Für die klassische IT übernehmen das bereits Security Operation Center (SOC). Die Medizintechnik hat hier noch einen Weg zu gehen. Der ist allerdings dringend notwendig, wenn man bedenkt, dass ein Krankenhaus ein Vielfaches an Medizintechnik im Vergleich zur Verwaltungs-IT betreibt.

Ein wichtiger Schritt ist somit die Anbindung der Medizintechnik an ein SOC. Passende Lösungen sind am Markt verfügbar. Nur so können Kliniken quasi in Echtzeit den Status der Cybersicherheit sämtlicher IT sichtbar machen. Und nur wer alles sieht, kann wirksame Cyberabwehr betreiben.

Olaf Janßen ist Leiter Information Security Management für die Geschäftsbereiche Public Sector und Healthcare Management von Sopra Steria.

Empfehlungen aus der Sicht des Auditors

KRITIS-Audits: Es geht um Glaubhaftigkeit

Audits für eine Krankenhaus-IT sind notwendig. Die Vorgaben, sie durchzuführen sind da. Und sie werden sich wie der regelmäßige TÜV-Termin fürs Auto (auch eine Art Audit) als Praxis einspielen. Es ist allerdings zu vermuten, dass die derzeitigen Schwellenwerte für die Durchführungspflicht nicht für immer Bestand haben werden, sondern der Kreis der Verpflichteten größer wird. Derzeit ist aber ein Audit noch für viele Klinikbetreiber Neuland, daher machen einige Tipps aus Sicht des Prüfenden Sinn. Von Stefan Stumm, lizenzierter Lead-Auditor

Generell kann man zwei Ansätze für die Vorbereitung von Audits erkennen: nur so viel Aufwand wie unbedingt nötig betreiben oder den Aufwand so gestalten, dass der maximale Nutzen aus dem ohnehin Nötigen gezogen werden kann. Der erste Ansatz ist bei Erstaudits üblich und verschiebt sich in der Regel immer mehr zum zweiten Ansatz, je mehr weitere Audits (zur Überwachung oder einer Re-Zertifizierung) durchgeführt wurden.

Wieviel Auditaufwand braucht ein Krankenhaus?

Für die Audits haben Krankenhäuser drei Optionen: den Branchenstandard, die Anwendung von ISO 27001 auf den Bereich oder ein eigendefiniertes Prüfverfahren. Das letztgenannte ist die deutlich aufwändigste Option, denn vor der Prüfung muss zunächst beschrieben werden, wie man prüfen möchte und anschließend möglicherweise diskutieren, ob das Verfahren so auch ausreicht.

Die beiden anderen Optionen sind sich inhaltlich relativ ähnlich: auch der Branchenstandard verlangt eine Anwendung der ISO 27001 auf den zu prüfenden Bereich, gibt aber einen definierten Prüfgegenstand vor, legt also fest, welche Komponenten der Krankenhaus-IT vom Grundsatz zu betrachten sind. Bei einer ISO-Zertifizierung legt das der Auftraggeber für die Prüfung – das Krankenhaus – selbst fest. Auch die Prüfregelmäßigkeit ist unterschiedlich, beim Branchenstandard alle zwei Jahre vollständig, bei der Zertifizierung alle drei Jahre, dazwischen jährlich ein Überwachungsaudit mit einem geringeren Prüfumfang.

Während der Umfang der Audits noch relativ ähnlich ist, gibt es größere Unterschiede im praktischen Nutzen. Das Auditverfahren nach dem Branchenstandard führt nicht zu einer Zertifizierung. Ein Zertifikat kann aber in einem Schadensfall ein wichtiger Nachweis für das Management sein, das Nötige getan zu haben, um den Schaden zu vermeiden. Es kann daher von einer Schadensersatzpflicht befreien. Außerdem ist es nicht auf einen definierten Anwendungsbereich beschränkt, es können also auch weitere Aspekte des Klinikbetriebes (meist mit wenig Zusatzaufwand) in den rechtlichen Schutz des Zertifikates einbezogen werden. Auch wenn keine zusätzlichen Aspekte bestehen sollte daher geprüft werden, ob eine Zertifizierung teurer ist und ob die gewonnene Rechtssicherheit diesen Mehraufwand nicht rechtfertigen würde.

Was erwartet der Auditor? Zunächst einmal, dass ein kontinuierlicher Verbesserungsprozess in den Schritten Planen – Umsetzen – Prüfen – Aktualisieren / Verbessern eingeführt ist. Dieser Prozess ist der unverhandelbare Kern der ISO 27001 und damit auch des Branchenstandards. Nach diesem Vorgehen sind dann die konkreten Anforderungen an die Informationssicherheit gemäß des gewählten Standards zu gestalten.

Bei einem Audits erwarte ich daher von den jeweiligen Auftraggebern, mir glaubhaft darstellen zu können:

- dass sie sich die erforderlichen Gedanken zur Ausgestaltung der Anforderungen gemacht haben,
- dass sie die dabei festgelegten Maßnahmen veranlasst haben,
- dass sie sich im nötigen Umfang davon überzeugen, dass die Maßnahmen auch umgesetzt und effizient gehalten werden und
- dass dabei alle für den Geltungsbereich anzuwendenden Anforderungen betrachtet wurden.

Es wird nicht erwartet, dass alle Anforderungen des gewählten Standards buchstabengetreu erfüllt sind. Es steht den Auftraggebern frei, auf die Umsetzung von Anforderungen zu verzichten, z. B. wenn diese ein Risiko beheben soll, dass im konkreten Umfeld gar nicht (war nie vorhanden) oder nicht mehr (wurde durch eine andere Maßnahme behoben) besteht. Oder sie legen fest, dass Risiken für eine gewisse Zeit (weil die Umsetzung der Gegenmaßnahme noch dauert) oder dauerhaft vom Management getragen werden. Im Audit prüfe ich dies, indem ich mir das Informations-Sicherheits-Konzept anschaue und nachlese, ob die festgelegten Abweichungen beschrieben, ggf. begründet oder in einen Risikobehandlungsplan übernommen wurden. Es muss dabei erkennbar sein, wer für die Umsetzung verantwortlich ist. Auch muss ein Nachweis vorliegen, dass die Auftraggeber selbst regelmäßige Prüfungen durchführen. Danach verifiziere ich durch Stichproben, ob die festgelegten Maßnahmen auch umgesetzt sind.

Für ein Audit sollten also ganz konkret bereitgehalten werden:

- die Umsetzungskonzepte für die einzelnen zu berücksichtigenden Anforderungsbereiche,
- die Anweisungen, wie die Konzepte umzusetzen sind,
- die Nachweise, wie der Geprüfte selbst die Umsetzung der Anweisungen überprüft hat und
- spätestens bei den Folgeaudits die Nachweise, dass und wie die Aktualität der Konzepte geprüft wurde.

Für alle diese Nachweise gilt die Grundfrage aller Auditoren: „WO STEHT DAS?“

Worauf achtet der Auditor?

Es geht beim Audit um Glaubhaftigkeit. Eine vollständige Prüfung aller Maßnahmen ist nicht vorgesehen, der Auditor muss davon überzeugt sein, dass die Auftraggeber den Grundprozess verstanden haben und korrekt anwenden. Das größtmögliche Problem bei einem Audit ist, wenn der Auditor den Eindruck gewinnt, dass er hinters Licht geführt werden soll. Deswegen klingeln bei mir (und wahrscheinlich bei allen Kollegen auch) die Alarmglocken, wenn ich während eines Audits feststelle, dass versucht wird eine erkannte Schwachstelle durch „Dokumentationskosmetik" unkenntlich zu machen. Meine Aufmerksamkeit ist während der dann folgenden Prüfungen noch größer als ohnehin schon. Deswegen ist Offenheit für mich das Vordringlichste, was ein Auftraggeber beachten sollte. Es folgen Vollständigkeit und Plausibilität der Dokumentation. Ein Audit besteht aus einer Dokumentenprüfung und einer Vor-Ort-Betrachtung des Prüfgegenstandes. Die Dokumentation sollte daher so aufgebaut sein, dass ein Externer (was der Auditor zwingend ist) sie auch nachvollziehen kann. Es müssen keine vollständigen Sätze sein, die gewählten Formulierungen oder Abkürzungen sollten aber allgemeinverständlich sein. Vor der Vor-Ort-Prüfung werden die Stichproben vom Auditor festgelegt und den Auftraggebern mitgeteilt. Es müssen ja für die Gespräche vor Ort die zuständigen Mitarbeiter eingeladen werden. Es ist nicht verboten und beschleunigt ein Audit, wenn die Auftraggeber die Dokumente noch einmal gegenlesen, eventuell sogar aktualisieren und möglicherweise zusätzlich von der Prüfung betroffene Mitarbeiter (über den eingeladenen Personenkreis hinaus) vorwarnen (Stichwort „Offenheit").

Was kann beim Audit schiefgehen?

In der Regel weniger, als die Auftraggeber befürchten. Wirkliche Hemmschuhe für ein erfolgreiches Audit sind eigentlich nur, wenn der Grundprozess nicht nachvollziehbar ist (zum Beispiel weil interne Prüfungen nicht dokumentiert wurden) oder für den definierten Geltungsbereich erforderliche Komponenten übersehen und deren Sicherheit deswegen nicht geregelt wurden. Hier ist eine Zertifizierung oder Anerkennung nur mit gutem Willen der Zertifizierungsstelle oder des BSI möglich – und mit Auflagen verbunden. Oder eben die fehlende Glaubwürdigkeit bei „Kosmetikverdacht".

Wurden Schwachstellen übersehen oder nicht angemessen behoben, fehlen Nachweise oder lassen sich Regelungen effizienter gestalten, führt dies in den meisten Fällen zu einer Prüffeststellung, die zu einem festgelegten Termin behoben sein muss, häufig zum nächsten regulären Audit-Termin.

Ob ein Auftraggeber eine Prüffeststellung als „schiefgelaufen" bewertet, hängt vom anfangs erwähnten Grundansatz ab. Wer nur auf Kosten achtet wird sich eher über die Zusatzausgaben ärgern, wer bereits einen Schritt weiter ist wird auch den Zusatznutzen erkennen.

Was sind meine allgemeinen Erfahrungen bei der Auditierung?

Audits sind Vorsorgeuntersuchungen. Sie sind manchmal unangenehm, ja lästig, kosten Zeit und Geld und stören die tägliche Routine. Nach der Untersuchung fühlt man sich aber beruhigt, wenn nichts Wesentliches gefunden wird. Und selbst wenn etwas gefunden wird ist das noch gut, weil man dadurch Probleme beseitigen kann, bevor ein Schaden eingetreten ist. Im Laufe der Jahre habe ich aber einen zusätzlichen Effekt wahrnehmen können. Wie erwähnt ist der zu prüfende Kern der Informationssicherheit ein kontinuierlicher Verbesserungsprozess. Der Zwang, sich mit diesem auseinanderzusetzen, führt häufig tatsächlich zu einer kontinuierlichen Verbesserung. Durch die erforderliche Dokumentation werden Abläufe effizienter, Planungsabläufe werden routinierter gehandhabt und die Notwendigkeit der Überprüfung führt dazu, dass Regeln erkannt und beachtet werden. Dadurch wird die Informationssicherheit tatsächlich verlässlicher und Schadensereignisse weniger oder zumindest weniger groß.

Aus Sicht des Auditors stellt sich das in der Regel so dar, dass man beim ersten Audit auf eine gewisse ablehnende Distanz und Vorsicht trifft. Nach und nach ändert sich dies in eine vertrauensvollere Haltung, weil die Geprüften erkennen, dass die Ergebnisse nicht schmerzen oder zumindest einem guten Zweck dienen. Irgendwann hat sich dann Routine im Umgang mit der Informationssicherheit eingespielt. Der Verbesserungsprozess wird nicht mehr „beachtet", sondern „gelebt", die einzelnen Schritte sind so verinnerlicht, dass sie alltägliche Praxis geworden sind.

Ab diesem Zeitpunkt verändert sich auch der Charakter des Audits. Der Auditor wird nicht mehr so sehr als Prüfer wahrgenommen, sondern als Gesprächspartner für die Weiterentwicklung der Informationssicherheit. Die Grundfragestellung verschiebt sich von „Müssen wir das machen?" zu „Wie machen wir das am besten?".

Stefan Stumm ist seit 1994 auf die Beratung zum IT-Grundschutz spezialisiert, ISO 27001-Auditor auf Basis von IT-Grundschutz seit es das Verfahren gibt. Kundenschwerpunkt ist der Bereich der Daseinsfürsorge (Kommunen, Versorger, Krankenhäuser und deren RZ-Dienstleister).
www.stumm-it-sicherheit.de

Wettbewerbsvorteil für Klinikbetreiber

B3S als Leitfaden für mehr IT-Sicherheit in Kliniken

Krankenhäuser, die zur „Kritischen Infrastruktur“ (KRITIS) zählen, sind laut IT-Sicherheitsgesetz verpflichtet, sich gegen Cyberattacken und Systemausfälle besonders zu schützen. Die Deutsche Krankenhausgesellschaft (DKG) hat dazu einen branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus vorgelegt, den das BSI im Oktober 2019 auch anerkannt hat. Er gilt für Kliniken ab einer vollstationären Fallzahl von 30.000 pro Jahr. Doch auch für kleinere Häuser empfehlen sich diese Vorgaben als Leitfaden für mehr Versorgungssicherheit. Von *Benedict Gross*, Continuity und Krisenmanagement, und *Hendrik Gollnisch*, *Kritische Infrastruktur und Sicherheitsmanagement, beide PwC Germany*

Gesetzgebung noch nicht abgeschlossen

Die Deutsche Krankenhausgesellschaft (DKG) hat dem Bundesamt für Sicherheit in der Informationstechnik (BSI) am 2. April 2019 eine erste Version für den „Branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus“ vorgelegt. Damit setzt die DKG das IT-Sicherheitsgesetz aus dem Jahr 2015 um, das allgemeine Anforderungen formuliert und KRITIS-Betreibern und deren Branchenverbänden auferlegt, branchenspezifische Sicherheitsstandards (B3S) zu erarbeiten. Die gesetzgeberische Entwicklung ist damit jedoch längst nicht abgeschlossen, die Regelungen werden sich im Bereich der Cyber-Security weiter verschärfen. Das gilt auch für mögliche Sanktionen: Für das kommende IT-Sicherheitsgesetz 2.0 wird bereits eine drastische Erhöhung der Geldbußen bei Verstößen diskutiert. Sie sollen dann bis zu 20 Millionen Euro betragen oder vier Prozent des weltweiten Unternehmensumsatzes, je nachdem welcher Betrag höher ist.

Grundlage für einen sicheren Klinikbetrieb

Krankenhäuser, die als kritische Infrastruktur (KRITIS) gelten, müssen in Zukunft regelmäßig den Nachweis erbringen, dass sie die von der DKG entwickelten branchenspezifischen Anforderungen (B3S) erfüllen. Doch auch kleinere Häuser können sich beim Thema Cyber-Security an diesem Standard orientieren, denn der B3S stellt einen durchdachten Leitfaden für Kliniken aller Größen dar, um die digitalen Nervenstränge ihres Betriebs zu schützen. Der Standard beschreibt umfänglich die Prozesse und Maßnahmen, um eine robuste Informationstechnik zu gewährleisten und damit die medizinische Versorgung und Gesundheit der Patienten sicherzustellen. Um ein Informationssicherheits-Risikomanagement (ISMS-Risikomanagement) zu etablieren, sieht der B3S für Kliniken, die zur kritischen Infrastruktur zählen, insgesamt 37 Management-Anforderungen vor. Dabei ist die Informationstechnik auch nach der sogenannten Kritikalität zu bewerten, also der Frage, ab welcher Zeitspanne der Ausfall eines Systems die medizinische Leistungserbringung einschränkt.

Wesentliche Kernpunkte

- Krankenhäuser, die zur „Kritischen Infrastruktur“ (KRITIS) zählen, müssen sich gemäß IT-Sicherheitsgesetz gegen Cyberattacken und Systemausfälle besonders schützen.
- Die Deutsche Krankenhausgesellschaft (DKG) hat für die Gesundheitsversorgung im Krankenhaus einen branchenspezifischen Sicherheitsstandard (B3S) vorgelegt.
- Der Standard BS3 beschreibt 168 Maßnahmen, die nötig sind, um eine resiliente Informationstechnik zu gewährleisten und die medizinische Versorgung und Gesundheit der Patienten sicherzustellen.
- Um die Versorgung der Patienten in jedem Fall aufrechtzuerhalten werden neben dem Schutz der IT-Struktur auch Patientensicherheit und Behandlungseffektivität als wesentliche Aspekte definiert.
- Die Anforderungen betreffen aktuell nur Kliniken ab einer Schwelle von 30.000 vollstationären Behandlungsfällen pro Jahr, empfehlen sich jedoch auch für kleinere Kliniken.

Für die Gefährdungsanalyse gilt ein Allgefahren-Ansatz, der sich nicht nur auf IT-Parameter beschränkt, sondern sämtliche Faktoren umfasst, die den Klinikbetrieb beeinträchtigen können. Aufgelistet werden 40 verschiedene Bedrohungsszenarien, Schwachstellen und mögliche Gefahren wie beispielsweise Elementarschaden und Stromausfall, aber auch Cyber-Attacken und menschliche Fehler.

Der B3S-Katalog empfiehlt insgesamt 168 Maßnahmen, die in Muss-, Soll- und Kann-Anforderungen untergliedert sind. Damit kann das Regelwerk für Klinikbetreiber als Leitfaden für die Praxis dienen wie auch als Grundlage für Kontrollen.

B3S-Standard reicht über Cybersicherheit weit hinaus

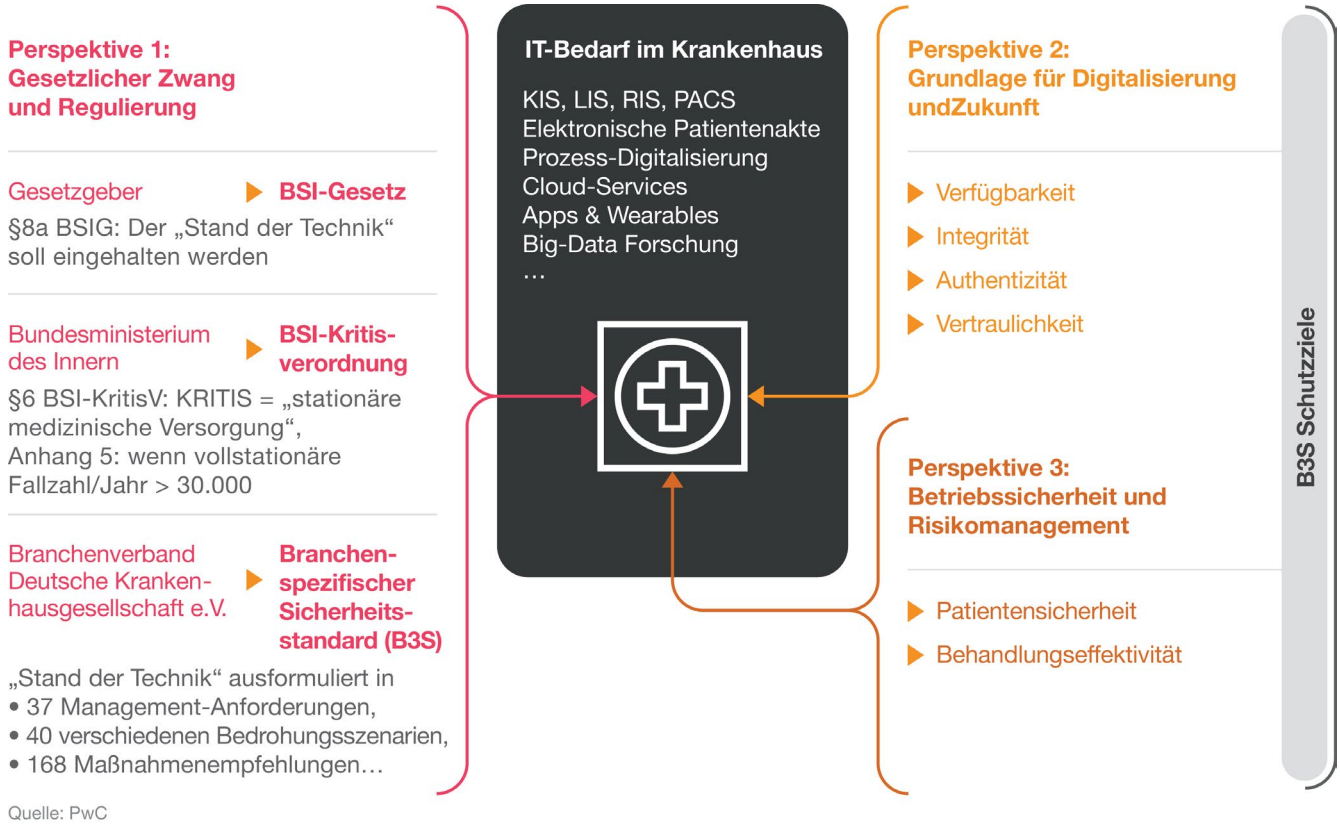
Auch wenn der B3S-Standard im Zuge des BSI-Gesetzes erstellt wurde, betrifft er nicht nur den Schutz der technischen Infrastruktur. Neben den vier klassischen Schutzzielen des Informationssicherheits-Managements (Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit) werden auch Patientensicherheit und Behandlungseffektivität als wesentliche Aspekte definiert. Der Standard zielt darauf, die medizinische Versorgung der Patienten zu gewährleisten, wofür die Informationstechnik eine grundlegende Voraussetzung darstellt. Neben technischen Aspekten werden deswegen auch die organisatorische, strukturelle und prozessuale Verantwortung auf Führungsebene genannt.

Der Standard verpflichtet beispielsweise auch die Geschäftsführung persönlich zur Bekanntgabe und Durchsetzung von Zielen der Informationssicherheit und fordert neben dem Datenschutzbeauftragten und der IT-Leitung einen dedizierten Informationssicherheitsbeauftragten (ISB bzw. CISO). Die Geschäftsführung muss notwendige organisatorische, personelle und finanzielle Mittel zur Verfügung stellen sowie die Wirksamkeit des Informationssicherheitsmanagements überprüfen und fortlaufend kontrollieren.

Versorgung auch bei Ausfall der IT gewährleisten

Die fundamentale Bedeutung von digitaler Informationsverarbeitung zeigt sich meist erst während des Ausfalls von Systemen. Damit in diesen Fällen die medizinische Versorgung – und somit das Krankenhaus als kritische Infrastruktur – aufrechterhalten werden kann, empfiehlt der B3S-Standard die Etablierung eines betrieblichen Kontinuitätsmanagement-Systems (Business Continuity Management). Dazu müssen zunächst kritische Systeme, Komponenten oder Prozesse mit hohem Risiko identifiziert werden. Für die Bereiche, deren Ausfall einen hohen Schaden verursacht, müssen Geschäftsfortführungs-, Notfall- und Wiederanlauf-Pläne erstellt werden. Diese Pflicht zur Identifizierung kritischer Leistungen in Verbindung mit der Gefährdungsanalyse im Allgefahren-Ansatz bildet die Grundlagen eines betrieblichen Kontinuitätsmanagements.

Der B3S beschreibt Anforderungen, die aktuell nur Kliniken ab einer Schwelle von 30.000 vollstationären Behandlungsfällen pro Jahr erfüllen müssen. Die Vorgaben dürften die meisten Häuser, die zur kritischen Infrastruktur zählen, vor große Herausforderungen stellen. Doch sie sind weder überzogen noch unerreichbar und in anderen Branchen schon lange Usus. Schließlich geht es nicht darum, formal einen Standard zu erfüllen, sondern die medizinische Versorgung der Patienten in jedem Fall aufrechtzuerhalten.



Quelle: PwC

IT-Sicherheit - für Klinikbetreiber als Wettbewerbsvorteil

Der B3S dürfte eine weitreichende Wirkung entfalten – vor allem im Zuge der steigenden Anforderungen und Sanktionen des geplanten IT-Sicherheitsgesetzes 2.0. Er gibt den Stand der Technik für informations(sicherheits)technische Prozesse so vor, dass er auch Krankenhäusern als Orientierung dienen kann, die nicht als kritische Infrastruktur gelten.

Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit bilden das strategische Fundament für die Digitalisierung von Versorgungsprozessen. Der B3S bietet deswegen auch die Chance, Mehrwert jenseits der gesetzlichen Pflichten zu entfalten. Ein gute Informationssicherheit kann zum Wettbewerbsvorteil für Klinikbetreiber werden, die Prozesse und Angebote digitalisieren und optimieren. Die Investitionen können sich auch im Hinblick auf zukünftige Digitalisierungsprojekte wie auch die Rechtssicherheit auszahlen.

Jedes Krankenhaus hat eine individuell gewachsene IT-Struktur

Der B3S der Deutschen Krankenhausgesellschaft spiegelt wider, wie heterogen und verflochten, aber auch wie individuell die Systemlandschaften in den einzelnen Einrichtungen gestalten. Wo in Krankenhäusern IT-Strukturen über Jahrzehnte gewachsen sind, sind die Spezialisten vollkommen damit ausgelastet, das Tagesgeschäft aufrechtzuerhalten. Zwischen dringlichen Anforderungen, personellen und finanziellen Grenzen bleibt kaum Zeit für eine langfristige strategische Planung. Für diese Häuser kann der neue Sicherheitsstandard im Zuge des BSI-Gesetzes den Anstoß zu größeren Veränderungen geben.

Doch auch Kliniken, die bereits nach bestem Wissen auf dem aktuellen Stand der Technik operieren, müssen überprüfen, ob und inwieweit sie dem B3S-Standard entsprechen:

- Im ersten Schritt sollten sie den Status Quo von Organisation und Technik analysieren und in Bezug zur kritischen Dienstleistung „medizinische Versorgung“ stellen.
- Durch den Vergleich dieser Status-Quo-Analyse mit den Anforderungen des B3S können im zweiten Schritt der Handlungsbedarf und die nötigen Investitionen ermittelt werden.
- Auf dieser Basis können Krankenhausmanagement und Betreiber eine kurz-, mittel- und langfristige Planung zur Umsetzung der B3S-Anforderungen entwickeln, die Gesamtkosten kalkulieren und belastbare Entscheidungen für Projekte treffen.

Maßnahmen und Empfehlungen von Experten

- Erhebung, Analyse und Beurteilung des Status Quo von Organisation und Technik sowie der vergleichenden Einschätzung hinsichtlich der Anforderungen des B3S
- Erstellung einer belastbaren Aufwandschätzung der nötigen Maßnahmen
- Entwicklung einer kurz-, mittel- und langfristigen Planung für die Umsetzung
- Ausgestaltung und operativen Einführung eines Informationssicherheitsmanagement-Systems (ISMS)
- Befähigung und Schulung des Informationssicherheitsbeauftragten
- Gestaltung und Einführung eines Business-Continuity-Management-Systems (BCM), einschließlich Notfallkonzeptionen, Wiederanlaufplänen sowie Tests und Übungen
- Beratung bei der Einwerbung von Fördermitteln für die Realisierung von Maßnahmen zur Umsetzung des B3S
- Auditierung Ihrer Organisation nach den Maßgaben des BSI-Gesetzes und des B3S

Benedict Gross, Continuity und Krisenmanagement, PwC Germany

Hendrik Gollnisch, Kritische Infrastruktur und Sicherheitsmanagement, PwC Germany

Digitalisierung: mit Standards zur Interoperabilität

FHIR erschließt für Anwender ganz neue Möglichkeiten

FHIR eröffnet Anwendern und Anbietern im Gesundheitswesen neue Chancen. Wie weit Krankenhäuser mit dem FHIR-Standard vertraut und wie FHIR-Produkte auf dem deutschen Markt bereits vorhanden sind, skizziert FHIR-Expertin Simone Heckmann, Geschäftsführerin / CEO, Gefyra GmbH.

Wie weit ist FHIR in Deutschland vorgedrungen? Wie sind Krankenhäuser mit dem Thema Vertraut? Wie weit zieht die Industrie mit?

Simone Heckmann: Das Interesse an FHIR ist derzeit enorm. Als Anbieter von FHIR-Schulungen spüren wir bei Gefyra seit einigen Monaten einen sprunghaften Anstieg der Nachfrage.

Wir sehen derzeit zweierlei Ursachen: Einerseits nimmt die Anzahl der Szenarien, in denen Hersteller FHIR-Schnittstellen in einem bestimmten Zeitraum umsetzen müssen zu. Hier sei zum Beispiel die KBV-Spezifikationen zur Archiv- und Wechselschnittstelle genannt.

Andererseits erkennen Hersteller aber auch den Nutzen von FHIR zu rein internen Zwecken. Zunehmend tritt FHIR anstelle von proprietären REST-Schnittstellen, wenn Hersteller zum Beispiel eigene Webapplikationen oder mobile Apps an ihre Back-End Infrastruktur anbinden wollen. Sehr häufig hören wir den Satz "das hätten wir vor zwei Jahren wissen sollen" wenn wir FHIR in Software-Unternehmen vorstellen. Die Entscheidnung, bereits implementierte, proprietäre Schnittstellen durch FHIR abzulösen, bringt mittelfristig zwar großen Nutzen, weil man mit den vordefinierten, wiederverwendbare Komponenten, die FHIR bietet, schneller enwickeln kann, aber die Ablösung bereits etablierter Lösungen kostet kurzfristig zunächst Zeit und Geld. Diese Umstellung in die Roadmap einzutakten, dauert daher einige Zeit.

In beiden Fällen, dringt FHIR derzeit aber noch nicht spürbar zum Anwender durch. Bisher ist der Kreis der Krankenhäuser, die sich intensiv mit dem Thema befassen auf die Universitätskliniken begrenzt, die FHIR im Rahmen der MI-Initiative für die Bereitstellung von klinischen Daten für die Forschung nutzen.

Doch das wird sich im Laufe des Jahres, wenn Cerner und SAP erste Produkte mit FHIR-Schnittstellen ausrollen, sicherlich ändern.

Simone Heckmann, Geschäftsführerin / CEO, Gefyra GmbH: „Mir ist es wichtig, dass die Krankenhäuser FHIR als eine Chance sehen, aktuelle Probleme und Herausforderungen wie z.B. Vendor-Lock-In, Patienten-Teilhabe und integration mobiler Anwendungen anzugehen und nicht nur als "schon wieder ein neuer Standard".

Welche Chancen bietet FHIR Anwendern sowie Anbietern im Gesundheitswesen?

Simone Heckmann: Der größte Zukunftspotential von FHIR ist die Wiederverwendbarkeit der einzelnen Bausteine des modularen Standards. Bisher haben Hersteller das Datenobjekt "Diagnose" etliche Male implementiert: Als DG1-Segment einer HL7 V2-Nachricht zum Versand an die Subsysteme, als CDA-Artefakt für den strukturierten Arztbrief, als CSV-Datensatz für die §301-Schnittstelle, als XML-Datei für die Krebsregistermeldung...

In FHIR kann ein und das selbe Objekt immer wieder verwendet werden, indem man es einfach "umverpackt". Mal als Bestandteil einer Nachricht, mal als Eintrag in einem struk-

turierten Dokument, mal als Teil eines Melde-Datensatzes.
Das erfordert natürlich eine Konvergenz der Technologie auf Seiten der Spezifikationen, die mittlerweile zwar in einigen, aber noch nicht allen Bereichen absehbar ist.
Weiterhin ist FHIR ein Standard mit einer großen und sehr aktiven weltweiten Community.
Die Verfügbarkeit von Code-Bibliotheken, Beispielimplementierungen, Open-Source-Servern und Testskripten macht FHIR - obgleich komplex - dennoch schnell implementierbar. Allein die Tatsache, dass sich ein Entwickler an die Community wenden kann, wenn ein Problem oder eine Frage auftritt und dort Gleichgesinnte findet, die eine Idee oder sogar eine Lösung parat haben, spart bei der Entwicklung viel Zeit.
Für die Anwender erschließt FHIR in Zukunft ganz neue Möglichkeiten, Softwaresystem zu individualisieren. Anstatt monatelang beim Hersteller eines KIS-, PVS- oder Subsystemes auf die Umsetzung eines gewünschten Features zu warten, macht es FHIR in Verbindung mit dem SMART-Framework möglich, einfach die App eines Drittherstellers zu integrieren, die diese Funktionalität abbildet. Das heute schon weit verbreitete Prinzip des "Fremdaufrufes" wird künstig ersetzt werden durch eine standardisierte, enge Integration webbasierter Lösungen in klinische Primärsysteme.
In anderen Industrie-Bereichen ist dieses Prinzip der "offenen API" längst üblich. Fast jede Branchenlösung kommt heute mit ihrem eigenen Appstore daher, über den sich gewünschte Zusatzfunktionen integrieren lassen, ob CRM-Syste, Buchhaltungssoftware oder Kollaborationsplattform. In kaum einer Industrie sind die funktionellen Anforderungen der Anwender so verschieden wir im Gesundheitswesen. Daher ist das Weiterdenken klinischer Primärsysteme zu offenen Plattformen eine längst überfällige Entwicklung.

Gibt es FHIR-Produkte auf dem deutschen Markt mit tatsächlicher Kompatibilität zum FHIR-Standard?

Simone Heckmann: Zunächst gibt es keine "tatsächliche Kompatibilität" zum FHIR-Standard. FHIR ist lediglich ein Framework, in dem vieles offen und fast alles optional ist. Dies ist auch einer der am häufigsten geäußerten Kritikpunkte an FHIR. Für einen internationalen, domänen-übergreifenden Standard, der in allen Bereichen des Gesundheitswesens einsetzbar sein soll, ist diese Offenheit jedoch eine notwendige Voraussetzung.
Kompatibilität entsteht in FHIR durch die Verwendung von Implementierungsleitfäden, die die Nutzung von FHIR in einem ganz konkreten Szenario beschreiben und die dafür erforderlichen Mindestanforderungen (Pflichtfelder, API-Funktionen, Terminologien) definieren.
Dieses Prinzip ist nicht neu. Auch CDA ist ein Standard, der erst durch die Erstellung eines Leitfadens konkret implementierbar wird. Für HL7 V2 waren es oft die IHE-Profile, die Interoperabilität zweier System gewährleisten konnten (man denke hier zum Beispiel an das Radiologische Order-Entry-Profil).
Was FHIR jedoch besser macht, als alle bisherigen Standards, ist die Tatsache, dass die Implementierungsleitfäden ein integraler Bestandteil des Frameworks sind. Sie sind nicht nur ein "Beipackzettel" sondern selbst standardisierte, maschinenlesbare Spezifikationen, gegen die man Instanzen unmittelbar auf Kompatibilität testen kann.
Solche konkreten Implementierungsleitfäden haben wir in Deutschland zum Beispiel in Form der KBV-Spezifikationen für die Verordnungs- und Archiv-/Wechselschnittstelle, oder der KV Telematik-Spezifikation für den eTerminservice, deren Umsetzung durch die Hersteller bis Ende 2020 erfolgen muss. Weitere Leitfäden aus der Feder der Medizininformatik-Initiative liegen inzwischen vor und werden derzeit durch die Hersteller, die an den Konsortien beteiligt sind, implementiert.

Wie können sich Anwender an der Weiterentwicklung beteiligen?

Simone Heckmann: Die wichtigste Form der Beteiligung ist das Mitreden! Auf der Internationalen Community-Plattform http://chat.fhir.org gibt es inzwischen vier verschiedene deutschsprachige Unterforen:

- "german(d-a-ch)" für allgemeine Diskussionen mir Relevanz im deutschsprachigen Raum,
- "german/mi-initiative" für den Austausch von Beteiligten an der Mi-Initiative,
- "german/kbv" für Entwickler und Anwender der KBV-Spezifikationen und
- "german/terminologie" für alle Fragen rund um die Auswahl und Nutzung von Terminologien.

Aus den Anforderungen der deutschsprachigen Community heraus gibt das technische Komitee von HL7 Deutschland regelmäßig Änderungs- oder Verbesserungsvorschläge in den internationalen Standard ein.

KH-IT-Frühjahrstagung „Digitalisierung: mit Standards zur Interoperabilität“

Charité: „*Health Data Plattform*“ unterstützt Patienten und Nutzer

Daten aus den diversen Hersteller-Silos zusammenzuführen und dabei sowohl besser zu strukturieren als auch internationale Standards für Datenformate zu nutzen, sind Herausforderungen an ein „neues KIS“. Die Charité Universitätsmedizin Berlin entwickelt dazu eine „Health Data Plattform“. *Dr. med. Peter Gocke, Chief Digital Officer (CDO), Leiter Stabsstelle “Digitale Transformation”, skizziert Konzeption, Aufbau und Perspektiven.*

Welche Herausforderungen stellt das „neue KIS“ und das Informationsmanagement an Industrie und Krankenhäuser? Wie weit sind sie darauf vorbereitet? Was ist noch zu tun?

Dr. Peter Gocke: Der KIS-Markt in Deutschland zeichnet sich im Moment durch viel Unruhe und vielfältige Besitzerwechsel aus – eine zukunftsorientierte und vor allem zügige Weiterentwicklung der Produkte ist dabei nicht erkennbar. An der Charité beobachten wir die Entwicklungen aufmerksam – auch in den europäischen Nachbarländern und international.

Um die eigene Digitalisierung auch unabhängig von KIS-Lieferanten voranbringen zu können, haben wir vor fast drei Jahren mit der Konzeption und dem Aufbau der sogenannten „Health Data Plattform“ begonnen, die es uns ermöglicht, Daten aus den diversen Hersteller-Silos zusammenzuführen und dabei sowohl besser zu strukturieren, als auch internationale Standards für Datenformate nutzen zu können – Stichworte sind hier u.a. Snomed CT, LOINC, UCUM, OMOP, HL7. Diese Plattform erlaubt bereits die Nutzung einzelner Algorithmen z.B. zur frühzeitigen Entdeckung von Patienten mit Niereninsuffizienzen – und wird konsequent weiter ausgebaut.

Dr. med. Peter Gocke, Chief Digital Officer (CDO), Leiter Stabsstelle “Digitale Transformation”, Charité Universitätsmedizin Berlin: „Digitale Medizin bedeutet eine sektorenübergreifende, gemeinsame Nutzung strukturierter Daten in Echtzeit – unterstützt durch Algorithmen und Module von künstlicher Intelligenz. Darauf müssen wir alle uns durch Anpassung unserer Technologie, aber vor allem unserer Prozesse und Strukturen vorbereiten. Digitalisierung ist auch eine Kulturfrage – und erfordert vor allem eine „informierte Kooperation“ aller (!) Beteiligten.“

Welche Kernpunkte bei Konzeption und Umsetzung von Plattformen für strukturierte Datennutzung sind besonders wichtig?

Dr. Peter Gocke: Die Antwort haben Sie schon in Ihrer Frage vorweggenommen: Es geht um strukturierte Daten, nicht um die Ablage und Kommunikation von PDFs (wenn „Daten das ÖL unseres Zeitalters" sind, ist die Gewinnung von strukturierten Informationen aus PDFs mit Fracking vergleichbar.) Vor allem sollten wir endlich damit beginnen, die Telematik-Infrastruktur und die darauf entstehenden Strukturen wie eine ePA zu unterstützen: wir haben hier eine Plattform, die das Potenzial hat, im deutschen Gesundheitswesen die sektorübergreifende Digitalisierung zu ermöglichen. Das bedeutet: bitte keine lokalen Vernetzungsprojekte mehr – auch wenn diese zunehmend handwerklich gut und nach IHE-Prinzipen aufgesetzt werden. Lieber diese Vernetzung auf Basis der TI vorantreiben – das kommt dann nicht nur lokalen Einrichtungen und deren Patienten, sondern uns allen zu Gute. Zuguterletzt sollte auch die europäische Facette nicht außer Acht gelassen werden, hier zeichnen sich in allen Mitgliedsländern Bestrebungen ab, Daten aus elektronischen Patientenakten übergreifend verfügbar zu machen (EHRxF - Electronic Health Record exchange Format). Hier sollten und müssen die gleichen Standards zur Interoperabilität zum Einsatz kommen wie in den nationalen Projekten.

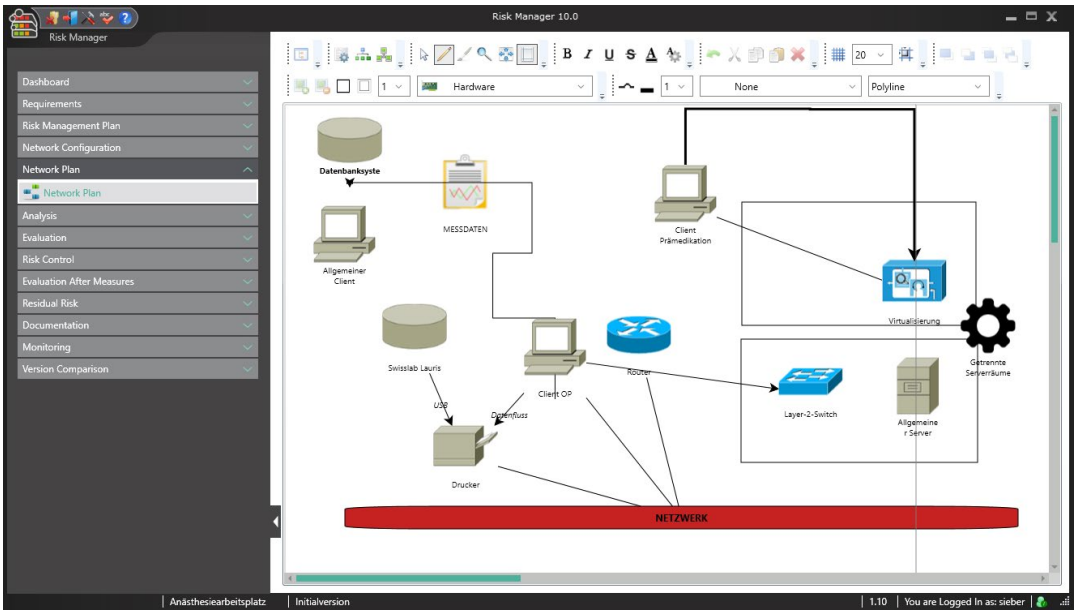
Wie ist bei der digitalen Transformation der Anspruch zu verwirklichen: „Die IT muss sich dem Nutzer anpassen, nicht umgekehrt"?

Dr. Peter Gocke: Diese Forderung hat in der Vergangenheit allzu oft dazu geführt, dass einfach papierbasierte Prozesse „elektronifiziert" wurden – was weder der Nutzerseite noch den Prozessen gerecht wird und das Potenzial einer Digitalisierung verschenkt. Ich glaube, der Anspruch muss eher sein, dass die IT sich den neu definierten Prozessen anpasst („IT follows Process") und damit auch die Nutzer*innen adäquat unterstützt.

Kritische Infrastruktur durch Betrachtung der IEC 80001-1 schützen

Risikomanagement vom IT-Netzwerk im Krankenhaus

Als Teil der unverzichtbaren sozialen Infrastruktur haben Krankenhäuser eine herausragende Bedeutung für den Bevölkerungsschutz, weshalb sich eine Vielzahl dieser Einrichtungen zukünftig ebenfalls den Anforderungen des IT-Sicherheitsgesetzes an ebendiese kritischen Infrastrukturen stellen müssen. Die Risikoanalyse, welche im Rahmen der IEC 80001-1 beschrieben ist, wird dabei eine wichtige Grundlage zur Erfassung und Bewertung einer tatsächlichen Bedrohungslage.



Die bereits seit 2011 europaweit gültige Norm IEC 80001-1 richtet sich an alle Betreiber von IT- Netzwerken mit integrierten Medizinprodukten. Im Zuge zunehmender Digitalisierung nehmen diese eine immer größere Bedeutung im Arbeitsalltag eines Krankenhauses ein. Um Daten klinikweit intern medizinischem Fachpersonal zur Verfügung zu stellen und/oder zentral zu speichern, werden Medizinprodukte immer häufiger in die Netzwerke eingebunden. Hierdurch werden beispielsweise Prozesse zur Bereitstellung von radiologischen Bilddaten oder die Navigation und Planung von Operationen, teils sogar zwischen räumlich entfernten Kliniken, unterstützt.

Neben den zahlreichen Vorteilen für die medizinische Versorgung bergen IT-Netzwerke in Zeiten schnell verändernder Sicherheitsanforderungen und zunehmenden Bedrohungen durch Cyberkriminalität ebenfalls neue Risiken und Herausforderungen. Die IEC 80001-1 soll an dieser Stelle dafür sorgen, dass vernetzte medizinische Systeme sicher und den Schutzzielen entsprechend arbeiten können. Hierfür werden Verantwortlichkeiten definiert und Pflichten beschrieben, welche zur Einhaltung der drei Schutzziele zu erfüllen sind:

- Sicherheit (Freiheit von unvertretbaren Risiken)
- Effektivität (Wirksame Behandlung und Gesundheitsmaßnahmen aufgrund der im IT-Netzwerk
- ausgetauschten Informationen)
- Daten- und Systemsicherheit (Schutz von Informationswerten,Vertraulichkeit und Integrität)

Essentiell für die Betrachtung dieser Kriterien ist die Planung, Durchführung und Aufrechterhaltung eines Risikomanagements über den gesamten Lebenszyklus des IT-Netzwerkes hinweg, von Integration bis Trennung der Medizinprodukte vom Netzwerk - eine umfangreiche, abteilungsübergreifende Aufgabe welche Mitarbeiter-Ressourcen dauerhaft beschäftigen kann. Eine dazu getroffene Verantwortlichkeitsvereinbarung regelt das gemeinsame Agieren und dient der Absicherung der Schutzziele.

Aufwandsreduktion durch Toolunterstützung

Damit die Aufwände in IT und Medizintechnik nicht durch das Etablieren eines Risikomanagements dauerhaft ansteigen, unterstützt der BAYOOSOFT Risk Manager als Prozessbeschleuniger bei der Erfüllung dieser Anforderungen.

Hierfür stellt die marktführende Softwarelösung neben der Erfüllung zahlreicher Normen für Medizinproduktehersteller seit 2015 eine Erweiterung für Betreiber von medizinischen IT-Netzwerken zur Verfügung. Klares Ziel liegt dabei in einer strukturierten Arbeitsweise nach Lebenszyklusphase. Mitarbeiter werden entsprechend der von der Norm geforderten wesentlichen Aktivitäten durch den Risikomanagement-Prozess geleitet: Risikoanalyse, -bewertung, - kontrolle, Neubewertung sowie Monitoring. Ergänzt durch eine selbstlernende Wissensdatenbank wächst das Wissen im Krankenhaus dabei Netzwerkübergreifend an. Die Informationen können organisationsweit den berechtigten Mitarbeitern verfügbar gemacht und häufig wiederkehrende

Elemente werden bei neuen Risikoanalysen bereitgestellt. Alle Anforderungen, Hersteller, Netzwerkkomponenten, Änderungen und Überwachungen werden an einer zentralen Stelle geplant und dokumentiert. So arbeiten IT, Medizintechnik und Risikomanagement effizient und zielgerichtet Hand in Hand. Gleichzeitig können mögliche Gefährdungen, die durch die Vernetzung der Medizinprodukte im IT-Netzwerk hervorgerufen werden, frühzeitig erkannt und reduziert werden.

Die Erfüllung der IEC 80001-1 ist bislang nur für die Krankenhäuser verpflichtend, welche als kritische Infrastruktur eingestuft wurden. Gleichzeitig dient die Einhaltung ihrer Prozesse der Reduktion von Haftungsrisiken und empfiehlt sich damit für alle Einrichtungen mit medizinischen IT-Netzwerken. Neben dem zentralen Punkt der erhöhten Sicherheit von Patienten und Anwendern zeigen sich hierbei insbesondere Vorteile in der Dokumentation und Transparenz, welche zukünftige Projekte schneller und zuverlässiger durchführen lassen. Die mit dem Prozess verbundenen erhöhten administrativen Aufwände lassen sich mit dem BAYOOSOFT Risk Manager deutlich reduzieren. Um einen Überblick über den Prozess und die Vorteile der Softwarelösung zu erhalten, bietet BAYOOSOFT derzeit eine kostenfreie Teststellung für das IT-Netzwerke Modul an. (www.riskmanager.net/it-netzwerke) Eine Evaluierung lohnt sich – nicht nur für die Aufwandsreduktion, sondern ebenfalls für den Schutz der sozialen Infrastrukturkomponente Krankenhaus vor potentiellen Cyberangriffen.

BAYOOSOFT Risk Manager

BAYOOSOFT, Business Unit der seit 2001 am Markt etablierten BAYOONET AG mit Sitz in Deutschland, ist Experte für Management Software Lösungen. Der Fokus liegt auf stark regulierten Bereichen und kritischen Infrastrukturen. Die, durch den TÜV Hessen nach ISO 9001 und ISO 13485 zertifizierten Qualitätsmanagementprozesse sind Ausdruck der Leidenschaft für nachhaltige Unternehmenslösungen und ausgeprägte Kundenorientierung. BAYOOSOFT ist Hersteller des Risk Manager, für die Generierung einer einwandfreien Technischen Dokumentation von Medizinprodukten und medizinischen IT-Netzwerken, sowie des Access Manager, Lösung für automatisiertes Berechtigungsmanagement.

Warum die Digitalisierung der Kliniken noch immer in den Kinderschuhen steckt

Von Dr. Djordje Nikolic

Es gibt mehrere Gründe dafür, warum sich derzeit so viele Kliniken in den roten Zahlen befinden. Die nur schleppend vorangehende Digitalisierung ist einer davon. Um die immer exorbitanter wachsenden Verwaltungsaufgaben zu stemmen, die Abläufe besser zu koordinieren und die vorhandenen Potenziale im Haus zu nutzen, haben viele Klinikgeschäftsführer jetzt zwar die Ausarbeitung eigener Digitalstrategien auf die Agenda gesetzt. Wer allerdings genauer hinsieht und nachfragt, erkennt schnell, dass kaum eine Klinik über eine wirklich klinikumfassende Digitalstrategie verfügt. Maximal gibt es derzeit Strategien und Konzepte für einzelne Bereiche als Insellösungen.

Hohe Priorität hat natürlich der Schutz der kritischen Infrastruktur der Kliniken, online und offline. Auf der Gewährleistung stabiler IT-Systeme und dem Schutz vor Datenverlust als Folge von Hackerangriffen liegt das Hauptaugenmerk. Um Kosten einzusparen wird vielerorts auch die Idee vom „papierlosen Krankenhaus" verfolgt. Bei der konsequenten Umsetzung dieses Vorhabens treten jedoch neben den eingeschränkten finanziellen Möglichkeiten die Anforderungen des Datenschutzes zunehmend auf die Bremse.

Mit ihren Digitalstrategien bewegen sich die meisten Kliniken also immer noch auf der rein operativen Ebene, eine wirklich strategische Ausrichtung der Digitalstrategie steht noch nicht im Vordergrund.

Es gibt aber auch einige Vorreiter und Vorbilder die aufzeigen, wohin die Reise geht. Kliniken, die mit einem ganzheitlichen Digitalisierungsansatz weit fortgeschritten sind, zeichnen sich in den meisten Fällen durch Merkmale wie beispielsweise folgende aus:

1. Der IT-Leiter ist Kulminationspunkt für Innovationskultur im ganzen Unternehmen und bremst neue Ideen nicht mit dem Blick auf das Budget aus.

2. IT-Mitarbeiter, klinische und administrative Anwender arbeiten nicht bloß in ihren jeweiligen Sphären nebeneinander her, sondern sorgen durch engmaschigen Austausch dafür, dass digitale Innovationen und neue Verfahren auch wirklich praktisch umgesetzt werden.

3. Klinikgeschäftsleitung und IT-Leitungsebene haben ein gemeinsames und konsentiertes Zielbild und legen ein hohes Maß von Intrapreneurship und Entscheidungsfreudigkeit an den Tag.

4. Die Wirtschaftsplanung umfasst neben den analogen Notwendigkeiten des Hier und Jetzt auch Investitionen in eine digitale Infrastruktur.

Digitale Projekte gründlich anzustoßen bedeutet für die Kliniken, dass sie all ihre über die Jahre eingespielten aber oft auch bereits aus der Zeit gefallenen Prozesse in Frage stellen oder komplett umwerfen müssen. Für viele Entscheider bedeutet ein solch rigoroses Einschreiten aber schlichtweg zu viel Aufwand, da sich schnelle Erlöse nicht garantieren lassen und sie Entscheidungen für längerfristige Erfolge und Kosteneinsparungen nicht verantworten wollen.

Es ist an der Zeit, dass Klinikmanager sich bewusstmachen, dass automatisierte und standardisierte Prozesse Personalressourcen und Kosten einsparen. Vor allem aber verringern sie Fehler, sparen Zeit und steigern den Patientennutzen. Daran führt kein Weg mehr vorbei. Für die positiven Effekte gibt es zahlreiche Beispiele. Fangen wir an mit der elektronischen Patientenakte:

Seit vielen Jahren ist sie als Buzzword in aller Munde, in vielen Kliniken aber noch immer keine Realität. Dabei ist der Nutzen so unstrittig – Doppelerfassungen von Unverträglichkeiten, chronischen Erkrankungen, bereits durchgeführter Diagnostik und ähnlichem könnten den Behandlungsprozess schneller, effektiver und kostengünstiger werden lassen. Vor allem aber könnte die Personalbindung im administrativen Bereich gesenkt, Fehler minimiert und die Patientenzufriedenheit gesteigert werden.

Elementares passiert auch abseits der Krankenhausflure: Die Digitalisierung von Nebenprozessen im Tagesablauf eines Krankenhauses (wie z.B. Einkauf und Logistik) ist für den Patienten zwar nicht sichtbar, erhöht die Versorgungsqualität aber ungemein. Gute Erfahrung gibt es beispielsweise mit der Nutzung barcodebasierter Artikelkennung und webbasierten Bestellprozessen. Sie erleichtern eine effiziente Verbrauchssteuerung, verhindern Engpässe bei der Versorgung und gewährleisten eine bessere Rückverfolgbarkeit von Produkten. Digitale Schranksysteme können zudem als virtuelle Assistenten die Logistik und den Einkauf entlasten und sorgen für einen effizienten Prozessablauf.

Das Tracking von Patientenströmen und Geräten kann zu einer optimalen Steuerung der Patienten während des Klinikaufenthalts beitragen. Hier gibt es neben RFID-Lösungen auch IOT-Ansätze, die mit Bluetooth arbeiten und nicht nur in Echtzeit zeigen, wo sich Patienten oder Geräte befinden, sondern beispielsweise anzeigen können, wie viel Sauerstoff noch in den jeweiligen Flaschen auf den Stationen ist. So können wertvolle Erkenntnisse gesammelt und viel Zeit gespart werden. Im Alltag ist das Suchen und Auffinden von Betten, Infusomaten, Sauerstoffflaschen und ähnlichem ein enormer Zeitfresser für das Personal. Zu wissen, wo sich welcher Patient gerade befindet, hilft der Disposition des Hol- und Bringedienstes, der dann seine Touren optimieren und Wartezeiten in kalten Fluren oder Vorräumen für die Patienten verringern kann.

Auch im direkten Umgang mit den Patienten erleichtern digitale Hilfsmittel den Alltag der Mediziner: Spezielle mit Barcodes versehene Armbänder zeigen Ärzten und Pflegepersonal auf einen Blick, welche Medikamente benötigt werden. Das leidige Durchwühlen der Patientenakte gehört damit der Vergangenheit an.

In einer ganzheitlichen Digitalstrategie darf zudem der gezielte Einsatz von Robotern und Künstlicher Intelligenz nicht fehlen. Roboter leisten hervorragende Dienste beim Auffüllen von Regalen oder dem Transport von Patienten und Waren. Doch nicht nur in der Krankenhauslogistik, sondern auch im Operationssaal spielen Roboter eine immer wichtigere Rolle:

Durch die Medien seit Jahren auch schon einem Laienpublikum bekannt, ist der Da-Vinci-OP-Roboter. Unter anderem aus Kostengründen wird dieser hierzulande erst in wenigen Kliniken und nur sehr gezielt eingesetzt. Dabei werden OP-Roboter zur Zukunft der Medizin gehören. Wer sich dieser Entwicklung verschließt, wird langfristig auf dem Klinikmarkt nicht bestehen können. Roboter-Unterstützung in der Pflege ist kein Science-Fiction mehr und gerade in Zeiten des Pflegekraftmangels eigentlich ein Muss.

Die Digitalisierung ist unaufhaltbar – gerade in der Medizin. Das Ziel bleibt dasselbe: Patienten medizinisch bestmöglich zu versorgen. Die Wege, dieses Ziel zu erreichen, werden sich ändern: Ärzte und Pflegekräfte werden auf digitale Unterstützung zurückgreifen können. Nur wer bereit ist, mitzuziehen und die richtigen Mitarbeiter für diese Herausforderung zu gewinnen oder zu qualifizieren, wird mittelfristig überleben.

Über den Autor: Dr. med. Djordje Nikolic ist Gründer und Geschäftsführer von consus clinicmanagement. Der Arzt und Betriebswirt war zuvor viele Jahre lang als Klinikgeschäftsführer in Krankenhäusern verschiedener Versorgungsstufen tätig. Er kennt daher Kliniken sowohl von der medizinischen als auch von der ökonomischen Seite.

Das Internet of Medical Things und wie man es absichert

Vernetzte Geräte gewinnen auch im Gesundheitswesen immer mehr an Bedeutung. So entsteht in diesem Bereich aus dem IoT das IoMT. *Jochen Adler* von Open Text erklärt, warum man sich jetzt mit der Technologie befassen sollte, wie Patienten und Dienstleister profitieren und welche Herausforderungen sich ergeben.

Prognosen zu Folge soll in diesem Jahr der Anteil der IoT-Geräte, die einen Gesundheitsbezug haben, 40 Prozent erreichen. Gleichzeitig existieren über 97.000 Gesundheits-Apps, denken Sie nur an den ständig wachsenden Markt der digitalen Services rund um Fitness- und Ernährung. Unser Gesundheitswesen erlebt eine rasche Digitalisierung, von der die Gesellschaft profitieren kann – wenn wir Sicherheit und Datenschutz nicht außen vor lassen.

Gesundheitssystem vor der Überlastung?

Wie in Deutschland auch, ist in den meisten Industrienationen die Lebenserwartung in den letzten Jahrzehnten konstant gestiegen; ein Ende dieses Trends ist nicht abzusehen. Während eine alternde Gesellschaft immer mehr medizinische und pflegerische Betreuung benötigt, fehlt es heute schon überall an Personal. Die pandemische Ausbreitung von Covid-19 hat schmerzhaft offengelegt, was Insider längst vorher wussten: Stress und Überlastung sind in Gesundheitsberufen oft die Regel. Eine weitere beunruhigende Entwicklung ist, dass es auf dem Land immer weniger niedergelassene Ärzte gibt und kleinere Kliniken vor der Schließung stehen, weil sie unrentabel geworden sind.

Vor diesem Hintergrund bleibt uns eigentlich gar nichts anderes übrig, als jede technische Lösung bereitzustellen und einzusetzen, die medizinische Berufe entlasten kann. Besonders Telemedizin spielt dabei eine Rolle. Eine Umfrage in den USA zeigte, dass dort 53 Prozent der Patienten eher einen Gesundheitsanbieter wählen würden, wenn dieser Remote- oder Telemonitoring-Geräte anbietet. Das erspart Menschen in ländlichen Gebieten lange Anfahrten zum Arzt, und kann dafür sorgen, dass niedergelassene Ärzte weniger Hausbesuche machen müssen.

Daten zusammenführen

Die Einführung vernetzter Geräte im Gesundheitswesen bringt jedoch auch einige Herausforderungen mit sich. Zunächst einmal bleibt es essentiell, das Vertrauen zwischen Patienten und Ärzten zu stärken, was angesichts der Fortschritte umso mehr technische Fortbildungen erfordert, aber eben auch Fingerspitzengefühl und Menschlichkeit. Nur so können Patienten auch das Vertrauen zu den Laboren und den Pharmaunternehmen aufbauen, dass notwendig ist, damit diese ihre Daten ohne Bedenken verarbeiten und weitergeben können. Diese realen Daten gilt es dann zu erfassen und mit anderen medizinischen Daten, zum Beispiel elektronischen Gesundheitsakten, zusammenzuführen, um Diagnosen und Therapien zu verbessern. Wenn solche Systeme implementiert werden, können im Gesundheitswesen viel Zeit eingespart und andernfalls explodierende Kosten eingedämmt werden. Auf der anderen Seite verursacht eine schlechte, brüchige Integration unnötige Arbeit. Systeme müssen künftig so konzipiert und realisiert sein, dass Messdaten, zum Beispiel aus Wearables wie Smart Watches, die längst auch EKG-Funktionen bieten, automatisch an die elektronischen Gesundheitsakten gesendet und dort gespeichert werden können.

Mit der Vertrauensfrage eng verknüpft ist zudem die Frage nach Cyber-Sicherheit. Im hiesigen Rechtsraum genießen Gesundheitsdaten – zurecht – besonderen Schutz. Medizin- und Gesundheitstechnik sind, wie viele andere Branchen auch, schon jetzt sehr anfällig für Datenverstöße. Die Verbreitung von IoMT-Geräten erhöht die Risiken von Verletzungen der Privatsphäre und sogar von Hackerangriffen dramatisch. Deshalb ist es notwendig, dass sich medizinische Institutionen auf die Umsetzung eines identitätsorientierten Ansatzes zur Sicherung und Verwaltung ihrer IoMT-Endpunkte konzentrieren.

Sicherheit im IoMT

Vermutlich nirgends kommt der Cyber-Sicherheit eine so entscheidende Bedeutung zu wie im medizinischen Bereich. Je nachdem, wie kritisch ein Gerät ist, könnten sogar direkt Menschenleben gefährdet werden. Das wäre etwa der Fall, wenn es gelänge, ein implantiertes Gerät, etwa einen Herzschrittmacher, von außen zu hacken. Doch auch außerhalb solch fataler Extremfälle ist die Sicherheit im IoMT von entscheidender

Bedeutung. Die erfassten Patientendaten gehören zu sehr sensiblen Informationen, die niemand in den falschen Händen sehen möchte. Eine Kompromittierung solcher persönlicher Daten hätte für Anbieter auch empfindliche rechtliche Folgen. Es steht also außer Frage, dass bei allen Überlegungen und Planungen bezüglich des IoMT Sicherheit an erster Stelle stehen sollte.

Allerdings sind gerade IoT-Geräte prinzipiell unsicher. Dort, wo die Hersteller für ihre Firmware auf die Nutzung von Komponenten aus freizugänglichen Open-Source-Bibliotheken verzichten und stattdessen proprietäre Lösungen implementiert haben, sind Schwachstellen im Code oft jahrelang versteckt – und im Extremfall ist das Wissen über solche „Exploits" auf einem florierenden Schwarzmarkt für Hacker zugänglich. Das müssen Verantwortliche bedenken, wenn sie Consumer-Geräte wie Wearables im medizinischen Kontext einsetzen möchten. Im schlimmsten Fall kann über ein einziges kompromittiertes Gerät ein ganzes Netzwerk infiltriert werden, beispielsweise im Krankenhaus. Aber, um beim einzelnen Patienten erheblichen Schaden anzurichten, reicht es schon aus, wenn Identitäten verwechselt werden, so dass beispielsweise die Dosierungen von Medikationen nicht mehr zur Person passen, was fatale Folgen haben kenn. Daher ist ein konsequentes Sicherheitskonzept für die weitere Verbreitung des IoMT so entscheidend, und deshalb braucht es ein Konzept, das auf gesicherten Identitäten basiert: Damit jederzeit aktenkundig ist, dass der IoMT-Sensor, der Messwerte übermittelt, auch tatsächlich zu der Person gehört, die ihm zugeordnet ist.

Folglich setzen verantwortungsbewusste Dienstleister im Gesundheitswesen auf einen identitätsbasierten Ansatz, der sich in anderen Bereichen bereits bewährt hat. Mit einer solchen Plattform ist es möglich, jedem Nutzer eine eindeutige Identität in Form eines digitalen Zwillings zuzuweisen. Dies wiederum erlaubt die anschließende Synchronisierung über alle Geräte, Anwendungen und sonstigen Ressourcen hinweg. Die Lösung erkennt außerdem neue Geräte, die sich mit dem Netzwerk verbinden, direkt. Sollte die Authentifizierung solcher Devices negativ verlaufen, können sie isoliert werden, schon bevor sie ihre ersten Daten übermitteln. Mit identitätsbasierten Plattformen erhalten Kliniken und andere Gesundheitsunternehmen ein digitales Abbild ihrer Netzwerkinfrastruktur, aber auch ein Netzwerk von „digitalen Zwillingen" aller Patienten. So lassen sich alle Beziehungen zwischen den verschiedenen Beteiligten darstellen, seien das Personen (Patienten, Ärzte, Pfleger), Geräte und Systeme.

Fazit

Vernetzte Geräte bieten ein großes Potential für die Medizin der Zukunft. Sie können dem Ärztemangel auf dem Land entgegenwirken und überlastetes Personal in Kliniken entlasten. Als Voraussetzung dafür muss allerdings Vertrauen geschaffen werden, was insbesondere eine solide Cyber-Sicherheit voraussetzt. Das muss für alle Akteure im Gesundheitswesen absolute Priorität haben.

Über OpenText

OpenText vereinfacht, transformiert und beschleunigt den Informationsbedarf von Unternehmen, auf der Basis von On-Premise oder Cloud-Technologien und schafft so die Voraussetzungen für die Digitale Welt.

Weitere Informationen über OpenText (NASDAQ: OTEX, TSX: OTEX) sind unter www.opentext.de auf dem Blog von CEO Mark Barrenechea verfügbar.

Jochen Adler von Open Text erklärt, warum man sich jetzt mit der Technologie befassen sollte, wie Patienten und Dienstleister profitieren und welche Herausforderungen sich ergeben.

Unentbehrlich analog

Unschlagbar digital

–

Heute.
Morgen.
Und in Zukunft.

–

agfahealthcare.de

AGFA HealthCare

KRITIS – Wege, Erfahrungen und Best Practices

Aus Gesprächen mit anderen Einrichtungen muss man feststellen, dass jeder Betreiber einer kritischen Infrastruktur im Krankenhausumfeld zum Thema KRITIS aus dem Audit zur Nachweiserbringung einen anderen Weg geht. Jeder Betreiber hat trotz gleicher Aufgaben- und Problemstellungen einen anderen Fokus und eine andere Zielsetzung, so dass jeder dieser Betreiber gerade für sich das Rad neu erfindet. Das sieht man auch an den aktuellen Diskussionen bei den Betreibern kritischer Infrastruktur im Krankenhausumfeld zu den verschiedenen Prüfgrundlagen. Die einen hatten beispielsweise zur Nachweiserbringung den Branchenstandard B3S als Prüfgrundlage und wollen zukünftig die ISO/IEC 27001 dafür als Grundlage nutzen und umgekehrt. Die Begründungen für den Wechsel der Prüfgrundlage sind oft nicht schlüssig und valide, kosten nur knappe Ressourcen und viel Zeit. Aufgrund der unterschiedlichen Prüfgrundlagen zur Nachweiserbringung sind auch die Ergebnisse zu ein und demselben Thema aus den Nachweiserbringungen komplett verschieden. Vergleichbarkeit zur Einhaltung „Stand der Technik" so nicht möglich.

Mitarbeiter-Awareness zur Informationssicherheit

Egal ob in Krankenhäusern oder anderen Branchen, die meisten erfolgreichen Zwischenfälle hatten überwiegend die Schwachstelle Mensch als Ursache. An erster Stelle muss in jedem Krankenhaus und Unternehmen die regelmäßige Mitarbeiter-Awareness zur Informationssicherheit stehen. Sämtliche bisher vorhandene Schwachstellen stehen mit dem menschlichen Handeln in Verbindung. Sei es, dass zum Beispiel die menschliche Neugierde ausgenutzt wird oder die menschliche Bequemlichkeit eine Ursache für technische- und organisatorische „Schlupflöcher" ist.

Auch ist in den Krankenhäusern aktuell zu erkennen, dass die Informationssicherheit noch kein fester Bestandteil der Krankenhauswelt ist. Bis dato liegt in vielen Krankenhäusern, die zur kritischen Infrastruktur gehören, der Fokus zur Informationssicherheit primär auf die Nachweiserbringungen. Die Aktivitäten zur Informationssicherheit im Krankenhaus haben bisher wenige Verknüpfungen zum täglichen Krankenhausbetrieb, sondern werden rein an die bevorstehende Nachweiserbringung oder an bevorstehende Audits geknüpft.

Was ist vor allem von den Krankenhäusern zu tun?

Informationssicherheit muss in den Krankenhäusern zukünftig zur unbewussten Kompetenz der Krankenhäuser dazugehören und das wird nur durch regelmäßige Awareness-Maßnahmen der Mitarbeiter im Unternehmen erreicht. Informationssicherheit muss in allen Krankenhausprozessen automatisch mit Berücksichtigung finden. Aufgrund der Überschneidungen zu den Themen: Datenschutz, Qualitätsmanagement/ Patientensicherheit, usw. mit der Informationssicherheit, sollten alle diese Bereiche im Krankenhaus eng verknüpft miteinander zusammenarbeiten und die Synergien gemeinsam nutzen, weil sonst die Gefahr besteht, dass thematisch gleiche Parallelstrukturen entstehen, die wiederrum kostbare Ressourcen im Krankenhaus binden.

Jens Schulze, KH-IT-Vorstand, schulze@kh-it.de

KRITIS – Erfahrungen und Best Practices

Seit 2015 gibt es den Branchenarbeitskreis (BAK) medizinische Versorgung innerhalb kritischer Infrastruktur (KRITIS). Der BAK wurde nach 2 Jahren Vorbereitung mit Unterstützung des KH-IT, DKG und des BSI gegründetseine Arbeit ist sehr aktiv und stetig.

Innerhalb KRITIS gibt es für die kritischen Sektoren unterschiedliche BAKs. Die Ziele der Branchenarbeitskreise sind die Interessen und Experten der IT-Sicherheit innerhalb des jeweiligen Sektors zu bündeln, um so die bestmöglichen Vorgaben und Verbesserungen für das Informationssicherheitsmanagement in der jeweiligen Branche zu erreichen.

Ich bin seit den ersten Schritten im Jahre 2013 dabei. Seit 2015 war ich stellvertretender Leiter und seit 2018 bin ich Leiter des Branchenarbeitskreis medizinische Versorgung. Im Beruf verantworte ich als CIO der ANregiomed die Strategie, Changemanagement, Betrieb und Prozessorganisation. Die ANregiomed versorgt mit zwei Grundversorgern, einem Schwerpunktversorger, einer Praxisklinik und mehreren MVZ den Landkreis und die Stadt Ansbach in Mittelfranken in Bayern.

Welche positiven Erfahrungen haben IT-Verantwortliche mit KRITIS bisher gemacht?

Ich persönlich habe bei dem Thema KRITIS die Erfahrung gemacht, dass Agieren besser ist als zu Reagieren. Es geht um die Informationssicherheit innerhalb des Unternehmens. Im Kern geht es um die Risikominimierung „eines Ausfalls" der kritischen Dienstleistung. Damit geht es um die Absicherung der Patientenversorgung. Der BAK ist dabei ein klarer Gestalter und bringt durch seine Experten entsprechende Handlungsempfehlungen raus bzw. gibt den nötigen Input für z.B. die Erstellung/Anpassung des B3S.

Die Erfahrungen kommen bei diesem Thema durch Angriffe und damit Störungen der kritischen Dienstleistung. Hierbei ist nicht die Ursache allein im Fokus. Vielmehr steht das Lernen daraus im Vordergrund:

- Was machen wir also, wenn es passiert?
- Wie gehen wir vor?
- Wer muss informiert werden?
- Welche Maßnahmen leiten sich ab?
- Was lernen wir daraus? etc.

Der BAK dient dabei als Plattform um Erfahrungen, Netzwerk und Hinweise zu bekommen.

In meiner persönlichen Wahrnehmung ist gerade die Mitnahme aller Mitarbeiter eine Herausforderung. Die Informationssicherheit macht die Systeme besser, jedoch ändern sich Abläufe und Prozesse. Der innere Schweinehund unser Mitarbeiter muss ausgetrieben werden. Hier müssen die Mitarbeiter eingebunden werden. Weiterhin muss man von positiven Erfahrungen berichten und Anreize schaffen.

Eine Wissenserweiterung bringt ein Penetrationstest innerhalb der Organisation. Dass es Lücken gibt, ist bekannt, jedoch wo und wie viele ist meistens eher im Verborgenen. Weiterhin lassen sich so den Mitarbeiter Beispiele besser darstellen.

Wo drückt der KRITIS-Schuh in Kliniken besonders?

Ein Thema ist die Finanzierung. Es gibt Seitens Bund entsprechende Strukturfonds. Jedes Bundesland hat dafür entsprechende Regelungen zum Abruf. Der Abruf erfolgt pro Bundesland unterschiedlich und die Finanzierung ist zum Großteil auf Investitionen ausgelegt. Bei Informationssicherheit geht es aber vor allem um den Betrieb, also um die Wartung und die dazu nötigen Ressourcen.

Ein weiterer Fokus liegt auf dem Änderungsprozess. Mit der Einführung eines neuen Systems bzw. Prozesses ist es nicht getan. Diese Änderungen benötigen Zeit und die Mitarbeiter müssen sich an die neuen Abläufe gewöhnen. Teilweise verlieren sie aus Sicht der Mitarbeiter entsprechende Flexibilität. Sie gewinnen aber an Sicherheit und das muss kommuniziert werden.

Was ist von den Krankenhäusern vor allem bei technischen und organisatorischen KRITIS-Maßnahmen und damit verbundenen Problemen zu tun?

Am 30.06.2019 war der erste Prüfnachweis von Häusern entsprechend des Schwellenwertes zu erfüllen. Alle zwei Jahre ist dieser zu erbringen. In dem Prüfnachweis geht es im Wesentlichen um eine Momentaufnahme und die Betrachtung von Risiken und Maßnahmen zu deren Reduzierung. Dieser Prozess bringt entsprechende Herausforderungen mit sich. Es beginnt bei der „Suche" nach einer prüfenden Stelle und endet bei der Umsetzung der jeweiligen Maßnahme. Durch die „erste" Welle der Prüfnachweise lassen sich Verbesserungen ableiten. Hier sind die Vorgaben z.B.

B3S aber auch Prüfnachweisdokumente zu verbessern. Der Branchenarbeitskreis hat gerade darauf seinen aktuellen Arbeitsschwerpunkt.

Die Herausforderungen in den Krankenhäusern sind die Umsetzungen aus den Maßnahmen. Die Umsetzung benötigt vor allem Zeit, welche abhängig von den verfügbaren Ressourcen sind. Auf der einen Seite müssen die Abläufe angepasst werden. Auf der anderen Seite werden Personalressourcen und Budgets benötigt. Somit kämpfen die Krankenhäuser um die Reihenfolge der Sicherheit, der Ordnungsmäßigkeit und der Wirtschaftlichkeit. Dieser Kampf muss gemeinsam auf der Führungsebene zusammen mit den jeweiligen Beauftragten abgestimmt werden und die Ergebnisse allen Mitarbeitern transparent kommuniziert werden.

Lars Forchheim, Mitglied im Vorstand des KH-IT, forchheim@kh-it.de

Kooperative Zusammenarbeit für einen sicheren IT-Betrieb

Cyber-Angriffe mit Ziel auf Software stehen im Vordergrund der Diskussionen. Wie sind Krankenhäuser gegen Attacken auf die physikalischen und elektrischen Eigenschaften bei Layer 1 geschützt? Dazu sind die Medizintechnik oder auch Beispiele für Cyber-Attacken mit manipulierter Hardware wie USB-Ladekabel, USB-Sticks, Modems oder Switches zu nennen, mit denen sensible Gesundheitsdaten ausgespäht oder gefährliche Skripte eingeschleust werden können.

Medizingeräte mit Netzwerkverbindung stellen zunehmend eine Gefahr für die IT-Infrastruktur, aber auch den Betrieb des Krankenhauses dar.

Während die IT-Abteilung unmittelbar Zugriff hat, auf die von ihr bereit gestellten Server, Speicher und Arbeitsplätze, und selbständig für die notwendige IT-Sicherheit sorgen kann, sind ihr im Bereich der Medizingeräte die Hände gebunden.

Problematisch sind vor allem die aufgrund des MPG vergebenen Geräteklassen, die wiederum nur wenig bis gar keine Änderungen an den jeweiligen Rechnern der Geräte zulassen. Dies fängt beim nötigen Virenschutz an und hört beim administrativen Zugriff nicht auf. Geschweige denn auch von der Möglichkeit USB-Ports zentral zu sperren oder Windows-Sicherheitspatches einzuspielen.

Damit sind Geräte in einem überwiegend sicher betriebenen Netzwerk am Laufen, die ähnlich einer Blackbox betrieben werden (müssen). Hinzu kommt, dass die Hersteller der Medizingeräte bzgl. der Windows-Versionen arg hinterherhinken. Ebenfalls kann es zu größeren Investitionen führen, wenn z.B. zwar eine Windows-10-kompatible Software zur Verfügung steht, die aber mit dem Gerät inkompatibel ist. Damit fallen dann nicht nur die Kosten für die Windows-10-Lizenz an, sondern auch u.U, mehrere Tausend Euro für den Ersatz des Medizingeräts. Investitionsmittel die bei kreativerem Design der Medizingeräte sinnvoller eingesetzt werden könnten.

Auch scheint es so, dass in den Gerätelisten der Medizintechnik für die Krankenhaus-IT notwendige Informationen fehlen, um z.B. nur den Migrationsbedarf zu ermitteln. Wenn Angaben zur eingesetzten Betriebssystemversion fehlen, müssen diese zunächst aufwendig erhoben werden.

Es ist dringend geboten, dass sich die Medizintechnik in kooperative Zusammenarbeit mit der IT-Abteilung begibt, um im Interesse des Krankenhauses einen sicheren IT-Betrieb der Medizingeräte zu gewährleisten.

Reimar Engelhardt, Stellvertretender Vorsitzender KH IT e.V.

Mitmachen: Resonanz ist Schlüssel zur Community

Sicher sind Informationen über den Verband noch zu verstärken, so über fachliche Kompetenz von Mitgliedern und Partnern aus Netzwerken in Fachartikeln. Auch in den neuen Medien wie Facebook etc. kann der KH-IT die Flagge noch etwas höher halten. Wie kann der KH-IT systematisch noch mehr Resonanz in der Fachöffentlichkeit bekommen?

Jens Schulze, KH-IT-Vorstand, CIO Universitätsklinikum Frankfurt/M. meint:

Der KH-IT kann nur durch seine Mitglieder (gerade außerhalb des Vorstands) mehr Resonanz in der Fachöffentlichkeit bekommen. Allein über bzw. durch den Vorstand und Einzelpersonen aus dem Vorstand ist das Flagge zeigen in der heutigen Welt nicht mehr möglich. Jedes Mitglied ist ein potentieller Markenbotschafter für den KH-IT. Wir können die Mitglieder aber nur als Markenbotschafter nutzen, wenn sie selbst in der Fachöffentlichkeit, in den sozialen Medien aktiv sind und über den KH-IT/ die Krankenhaus-IT bzw. als KH-IT-Mitglied/ Verantwortliche der Krankenhaus-IT kommunizieren. Genau das passiert leider zu wenig oder wird nicht von den Mitgliedern praktiziert. Viele Kolleginnen und Kollegen ziehen sich lieber in die Komfortzone zurück, anstatt einen Schritt aus der Komfortzone heraus zutreten und einfach mal andere neue Wege zu gehen oder andere neue Ansätze auszuprobieren.

Als Vorstandsmitglied fällt mir auf, dass innerhalb des KH-IT regelmäßig ein guter Austausch/eine gute Kommunikation innerhalb des Vorstands zu aktuellen Themen stattfindet, wir jedoch in der Regelmäßigkeit als Verband nicht optimal mit allen Mitgliedern zu den aktuellen Themen kommunizieren und uns gemeinsam austauschen. Das liegt u.a. auch daran, dass die Mitglieder unsere bestehenden Kommunikationsmöglichkeiten (Webseite, XING-Gruppe, Twitter, Facebook, etc.) nicht aktiv nutzen.

Ich hatte mir beim Initiieren des HK-IT-Twitter-Accounts und der KH-IT-Facebookseite vorgenommen, einzelne KH-IT-Mitglieder zu aktuellen Themen zu interviewen (ggf. als Podcast) und diese Interviews als Diskussions-/Newskonsum in den Medien zur Verfügung zu stellen. Nur mir allein fehlt die Zeit dazu, auch regelmäßig die sozialen Medien mit Content zu bestücken. Das muss durch mehrere Leute, mein Wunsch - durch die Mitglieder als Markenbotschafter – passieren.

Jens Schulze, KH-IT-Vorstand, schulze@kh-it.de

Rückblick auf den Health IT-Talk vom 19. Februar 2020 in Nürnberg

Andreas Henkel, CIO des Klinikum rechts der Isar der TU München

Gastgeber war die Bechtle Systemhaus Nürnberg GmbH in deren kürzlich neu bezogenen Räumlichkeiten. Der Referent des Bechtle GmbH IT-Systemhaus Nürnberg, CIO Bernd Cichon, trug das Vorgehensmodell der Bechtle für die Transformation von Digitalisierungsprojekten vor. Das Modell ist hersteller- und technologieneutral und in sechs modular aufgebaute Phasen aufgeteilt. Es erlaubt die unterschiedlichen Technologiebereiche auf die individuelle Kundengröße anzupassen. Die einzeln vorgestellten Phasen werden dokumentiert und dabei auf Vollständigkeit und Inhalt geprüft. Fehlende Teile werden dadurch identifiziert und im Laufe der Bearbeitung ergänzt. Der Kunde erhält nach jeder Phase die erstellte Dokumentation mit den erarbeiteten Ergebnissen. Ergänzt mit dem Hinweis auf so genannte Quick-Wins um den Reifegrad seiner IT zu erhöhen. Das Bechtle Consulting Modell kombiniert die unterschiedlichen Branchenkenntnisse der Business Architekten mit dem übergreifendem technischen Know How der Solution Architekten zu einer effizienten Symbiose für den Kunden.

Den Hauptvortrag hielt Andreas Henkel, CIO des Klinikum rechts der Isar der TU München. Herr Henkel zeigte die Herausforderung auf die in der Zukunft für die Krankenhäuser bestehen und hat speziell ein Konzept vorgetragen, wie Interoperabilität und eine Plattformstrategie für den Umbau der KAS/KIS-Landschaft eine wichtige Rolle spielen. Die Rahmenbedingungen am Standort München sind besonders herausfordernd, da der Erfolg der Weiterentwicklung in der Digitalisierung auch an der Gewinnung und dem Halten von gutem Personal hängt. Auch bestehen Unwägbarkeiten aus unklarer Finanzierungssituation. Hierüberhinaus sind wichtige Prinzipien durch die Softwareindustrie mit der Unterstützung offener Standards eine wichtige Grundvoraussetzung für das Gelingen eines barrierefreien Datenaustausches und damit für die Digitalisierung für zukünftige medizinische und pflegerische Prozessunterstützung, bei denen der Patient zukünftig mit der ePA die gewünschte Unterstützung erhält.

Leider musste die Organisation wie in anderen Regionen spüren, dass das Interesse von Vertretern der Industrie zu den angebotenen Vorträgen viel höher war, als das der Kollegen/innen aus den Krankenhäusern. Die Frage ist unbeantwortet ob es an den Themenstellungen lag oder ob andere Gründe dafür gesorgt haben, dass die Resonanz aus den Kliniken so gering war. Trotzdem haben sich zwei Teilnehmer bereit erklärt die nächste Veranstaltung zu planen. Wir hoffen, dass bei der nächsten Veranstaltung die Teilnehmeranzahl aus den Kliniken sich erheblich steigern wird?

Der nächste Termin wird voraussichtlich in den KW 29 oder 30 stattfinden. Gastgeber wird qSkills sein, der Kooperationspartner des KH-IT e.V. zu KRITIS-Schulungen.

Der Führungskräfte-Kongress Meeting-am-Meer 2020

Digitale Realität schaffen für Klinik und Patienten

Einblicke in die Krankenhaus-Praxis, Impulse der Lösungsanbieter – die Big Points, waren Inhalt des Meetings am Meer 2020. Dabei standen der digitale Patient und digitale Services im Mittelpunkt der Führungskräfteveranstaltung in Heiligendamm an der Ostsee. Was ein künftiges Krankenhaus auszeichnet, definierten Experten, Wissenschaftler und Praktiker. Sie gaben Klinikverantwortlichen konkrete Handlungsempfehlungen für die digitale Transformation und ihre Umsetzung: Was lohnt - und was nicht? Veranstalter war Prof. Dr. Wolfgang Riedel, Institut für Krankenhauswesen – IfK.

Weniger Bürokratie, effizientere Prozesse, höhere Mitarbeiterzufriedenheit, mehr Zeit für wertschöpfende Aufgaben und Patienten, bessere Medizin und eine bessere Behandlung – dadurch wird sich das Krankenhaus der Zukunft auszeichnen. Inspiriert von digitalen Trends können technische Innovationen auch im Krankenhaus einen wertvollen unterstützenden Beitrag zur Bewältigung akuter und kommender Herausforderungen leisten.

Prozesse und Strukturen im Krankenhaus der Zukunft werden automatisiert, digitalisiert, integriert und vernetzt, Entscheidungen werden dezentralisiert und autonom getroffen. Vision und Realität nähern sich an. Dazu bedarf es drei Voraussetzungen: IT-Infrastruktur, qualifizierte Fachkräfte und eine ganzheitliche Digital-Strategie.

ehealth-Trends, neue Player

Wie sich auch die Landschaft der IT-Lösungsanbieter ändert, verlagert sich die Position der Kliniken durch Vernetzung der Akteure. Sie stehen nicht mehr im Mittelpunkt. Künftig ist es der Patient, der den Ton angibt. Zugleich gewinnen die Patienten-Daten in nicht nur Kliniken an Bedeutung. Diagnostik, Behandlungsvorschläge, Therapieüberwachung etc. erfolgen in Zukunft datengestützt. Dieser digitale Wandel ruft neue Player auf den Markt. Zu den IT-Giganten zählen Alphabet. Facebook oder auch Microsoft. Start-ups belegen entscheidende Plätze. Diese neuen Akteure erlangen die Hoheit über die Patientendaten und die sie analysierenden KI-Systeme. Auf Big Data werden völlig neue Geschäftsmodelle basieren. Der medizinische Fortschritt wird den Fokus von einem tendenziell eher krankenheitsorientierten auf ein gesundheitsorientiertes System legen.

Hemmschwellen für Digitalisierung

Was die Digitalisierung in Deutschlands Kliniken hemmt, ist bekannt. „Föderale Politik als Hemmnis des Strukturwandels, unterfinanzierte Krankenhäuser und kaum digital vorbereitete Krankenhäuser mit CEO voller IT-SKepsis", postulierte Prof. Riedel. Und weiter: Veraltete ITK-Strukturen, viele Netze, aber wenig Internet Protokolle, kurz Prozesse wie vor 50 Jahren. Dem Personal fehlen IT-Kenntnisse, es mangelt an der Wertschätzung für Digitalisierung. Grund ist wohl, dass der Nutzen monetär oft schwer bewertbar und refinanzierbar ist, Vorteile ergeben sich oft erst längerfristig. (Hören Sie das Interview mit Prof. Riedel.)

Digitale Zukunft für Kliniken

Neue Strategien für Digitalisierung und herkömmliche IT-Konzepte infrage zu stellen sind für Kliniken überlebenswichtig. „Ohne zusätzliche Investitionsmittel wird dies nicht funktionieren, es zahlt sich aber bei richtiger Auswahl der Schwerpunkte schnell aus",meinte Dr. Frank Wartenberg, IQVI. Dabei zeigten sich Einsparpotentiale, etwa im Pflegebereich. „Zu Kernpunkten zählen vereinfachte Arbeitsabläufe und individualisierte Medizin. Hierbei spielen moderne digitale Services für Patienten eine entscheidende Rolle." Die digitale Zukunft für Kliniken in Deutschland bedeutet: Jedes Haus muss eine individuelle IT-Strategie für sein Zielkonzept erstellen. Dazu sind die vorhandene Umgebung und die Möglichkeiten zur Optimierung von Prozessen und medizinischer Datenhaltung zu berücksichtigen. Digitalisierung wird künftig zum Wettbewerbsfaktor im Gesundheitswesen. (Hören Sie das Interview mit Frank Wartenberg.)

Vom KIS zum Smart Hospital

Die IT muss sich den neu definierten Prozessen anpassen und damit auch Nutzer entsprechend unterstützen. Vorwärtsweisend ist es, Daten aus den unterschiedlichen Hersteller-Silos zusammenzuführen und dabei sowohl besser zu strukturieren als auch internationale Standards für Datenformate zu nutzen. Nach wie vor sehen sich jedoch Nutzer in Krankenhäusern mit Systemarchitekturen konfrontiert, die die interdisziplinären medizinischen und organisatorischen Prozesse behindern, anstatt sie zu verbessern. Die Vielfalt von Applikationen sorgt zum einen für hohen administrativen sowie technischen Aufwand. Zum anderen erhöhen Faktoren, die sich durch Komplexität von Systemen ergeben, die Risiken im Bereich der Informations- und Datensicherheit, der Anwenderfehler sowie der möglichen Inkompatibilitäten von Systemschnittstellen und Datenformaten. Diese Faktoren behindern den digitalen Prozess und können ihn nicht selten zum Erliegen bringen.

Einer der möglichen Gründe: „Bei digitalen Transformationsprojekten lassen sich häufig fehlende Strukturen beobachten", bemängelte Prof. Dr. Thomas Jäschke, FOM Dortmund.

Das Digitale Krankenhaus in Deutschland – vom KIS zum Smart Hospital
Der digitale Patient – neue Strategien und Lösungen mit digitalen Patientenservices
Prof. Dr. Wolfgang Riedel, IfK Braunschweig

„Die Prozesse sind vielfach nicht transparent, doch erst dadurch kann es zu einer Optimierung kommen", ergänzte Hendrick Riedel. Digital Avantgarde. Beide Experten unterstützen daher Krankenhäuser bei der Strategieentwicklung. Sie betonten: Erforderlich seien strukturelle und prozessuale sowie auch kulturelle Veränderungen. Ziele sind bessere Transformationsfähigkeit, schnellere Anpassung und erfolgreiche Innovationen.

Change Management - Bereitschaft zur Veränderung

Den Fokus bei digitalen Innovationsprogrammen und innovativen Projekte beschrieb Prof. Riedel. „Am Anfang neuer Digitalisierungsstrategien sollte immer eine Bewertung der heutigen Prozesse in Kliniken stehen." Die Bereitschaft zur Veränderung mangelhafter Prozesse und dem Einsatz digitaler Lösungen und Techniken ist der nächste Schritt, nicht umgekehrt. „Nicht Software und Hardware sind Maßstab für modernes IT-Management, vielmehr optimale Prozesse für Personal und Patienten. Hier sind ganzheitliche Strategien gefragt. Dabei sollte nicht jede Klinik alles neu erfinden, sondern vielmehr auf bewährte Standards setzen." Und immer wieder sollte der Anwender bei einer Digitalisierungsstrategie im Blick stehen. Seine Erfahrungen dazu gab Torsten Emmerich aus dem St. Johannes-Hospital Dortmund, an die Krankenhausverantwortlichen weiter. Er merkte an: „Zu den Problemen der Prozess-Digitalisierung gehört die Verschiebung der Arbeit zu Lasten anderer, also wenn ein Bereich viele Prozess-Schritte tun muss, jedoch damit ein anderer davon profitiert." Torsten Emmerich empfahl, hier das Gleichgewicht zu schaffen. (Hören Sie das Interview mit Torsten Emmerich.)

Durch IT die Pflege entlasten

Es gibt offenbar einen Mangel an Pflegefachpersonen, aber besonders einen Mangel an gut ausgebildeten Pflegenden, die unter den aktuellen Bedingungen noch bereit sind, zu arbeiten. Eine Optimierung der Arbeitsabläufe ist nötig. Digitale Anwendungen sollen den Arbeitsalltag vereinfachen. Heiko Mania geht es darum, Aufwände durch IT von der Pflege fernzuhalten. „Ein digitalisierter Pflegeprozess kann die Pflege nicht nur entlasten, er macht die Pflege messbar, steuerbar, effizienter und sicherer," ist der Geschäftsführer NurseIT Institute sicher. Wie sich nämlich zeigt, verlangen Pflegefachkräfte digitale Unterstützung wie beispielsweise Closed-Loop-Medication. „Mit einer Pflege-Expertenplattform sichert sich die Klinik zusätzliche Erlöse und steigert die Attraktivität des pflegerischen Arbeitsplatzes." (Hören Sie das Interview mit Heiko Mania.)

Strategie und Leuchtturmprojekte

Die Rolle der Kliniken im digitalen Gesundheitswesen wandelt sich. Digitales Krankenhaus, Smart Hospital und digitaler Patient - dabei kann das Management seiner Rolle in der digitalen Transformation gerecht werden kann, wenn sie diese aktiv vorantreibt und ein zukunftweisendes Mindset etabliert. Informrmations- und Kommunikationstechnik im Krankenhausbereich gehören zu den strategischen Faktoren. Big Points einer IT-Strategie verlangen das Personal aller Berufsgruppen früh einzubinden, Leuchtturmprojekte auszuwählen und zu realisieren, wobei es zunächst um ein digitales Teil-Krankenhaus geht, also nicht gleich ein ganzes Haus umzustellen. Dabei verbindet Software Patienten, Familien und Ärzte am Behandlungsort und darüber hinaus miteinander. (Hören Sie das Interview mit Prof. Dr. Bertram Häussler, IGES Institut.)

Nur wenige Krankenhausdirektoren sind IT-affin. Ein Beispiel ist Krankenhausdirektor Bernhard Ziegler, Klinikum Itzehoe. Sein Credo: „Wirtschaftliche Zwänge und ein sich verschärfender Personalmangel erfordern neue IT-Strategien." Der Manager führte Nutzenbeispiele durch Digitalisierung auf. Zugleich unterstrich er die Balance zwischen Nutzen und Kosten. „Nicht zuletzt ist moderne Technik Anreiz und Wett-

bewerbsvorteil, gerade für rare Fachkräfte.“ (Hören Sie das Interview mit Bernhard Ziegler.)

Mit „Deutschland und Europa in Zeiten von Globalisierung und Digitalisierung“ stellte Wolfgang Bosbach, MdB a. D., den großen Zusammenhang her. Er blätterte einen ganzen Strauß von brisanten Aspekten auf, von Globalisierung und Umweltproblemen über Brexit bis zu internationaler Diplomatie. Topic war ebenfalls Digitalisierung. Sie bewegt seiner Ansicht nach das Gesundheitswesen. Der Politiker mahnte kritisch: „Wir verlieren den Blick auf den wirtschaftlichen und sozialen Zusammenhang. Hier treffen Digitalisierung, Ökonomie und Gesundheitswesen zusammen. Es ist mit Blick auf die unterschiedlichen Interessenslagen eine falsche Annahme, dass der Markt es richtet.“ Und Bosbach resümierte: „Gesundheit wird teurer.“

Mut zur Patienten-IT

Digitalisierung für Anwender im Krankenhaus, Einblicke in die KH-Praxis, Impulse der Lösungsanbieter – die Big Points, waren Inhalt des Meetings am Meer 2020. Management und Digitalabteilungen können als Innovatoren neue Potenziale für nachhaltige digitale Lösungen im Diagnose- und Therapieprozess identifizieren. Online-Plattformen für die künftige Hauptperson bekommen hohe Bedeutung: Wichtig ist , den „Kunden“ Patienten über den Behandlungsverlauf zu informieren, den Patientenkomfort und die Patientenzufriedenheit zu steigern. Digitalisierung der Krankenhäuser – warum tun sich die Kliniken so schwer? Antworten beim Meeting am Meer waren vielschichtig und erhellend. Zu Digitalisierung und Prozessunterstützung gehört nicht zuletzt eine gewisses Maß an Mut: „Damit lässt sich nachhaltige Wertschöpfung ermöglichen, gerade bei digitalen Services rund um den Patienten“, betonte Veranstalter Prof. Riedel.

www.meeting-am-meer.de

Health-IT-Talk Berlin Brandenburg über IT im Krankenhaus

Regionale Grundversorger am digitalen Abgrund

„Wenn man den Medien-Berichten und Aussagen der Berater folgt, dann sind Krankenhäuser überwiegend nicht digitalisiert und was die Datensicherheit angeht ohnehin jenseits von Gut und Böse.“ Für Michael Thoss, IT-Leiter Klinikum Hochrhein, Autor und freier Berater, Mitglied im BV KH-IT, es ist Zeit, im Health-IT-Talk einmal „denkanstößig“ über die Realität der Informationstechnik zu reden. Klar ist: Durch erhebliche Hemmschwellen stehen kleinere Krankenhäuser, das Management und der IT-Leiter am digitalen Abgrund.

In den Medien wird ständig das Thema "Digitalisierung" im Gesundheitswesen der Krankenhäuser thematisiert als würde in den deutschen Kliniken die Bronzezeit gerade ausklingen und immerhin die Dampfmaschine 2.0 die Ablösung darstellen. Ein Wunder, dass die stationäre medizinische Versorgung überhaupt noch funktioniert und erstaunlich, dass mehr Behörden von Cyber-Vorfällen betroffen sind als Krankenhäuser.

Referent Michael Thoss überlegte: Was ist eigentlich Krankenhaus-IT, welche Komponenten müssen wir betrachten, wenn wir über "Digitalisierung" reden? Was versteckt sich insgesamt an Technologien und Aufgaben hinter solch vermeintlich simplen Begriffen und wofür müssen wirtschaftliche Mittel in der Realität primär aufgewendet werden? Viel wichtiger aber: „Woran hängt die vermeintlich nicht vorankommende Digitalisierung wirklich?“

In den klinischen Fachabteilungen eines Krankenhauses gibt es kaum noch Prozesse, die nicht direkt oder indirekt von IT-Systemen unterstützt werden. Anwenderzufriedenheit, also meist die wahrgenommene Benutzerfreundlichkeit der klinischen Applikationen, stellt ein wesentliches Qualitätskriterium einer professionellen Krankenhaus-IT dar. Sie ist zugleich essentiell für das Betriebsklima und im Endeffekt entscheidend für die möglichst optimale Patientenversorgung sowie Erlössicherung im Krankenhaus.

Im Vortrag ging Michael Thoss auf die aktuelle Situation und Lage der Grundversorger sowie die bestimmenden Faktoren und Rahmenbedingungen der "Digitalisierung" für kleine Krankenhäuser ein. Dabei eröffnete er den über 40 Health IT Talk-Teilnehmern die Gelegenheit, einen Blick hinter die Kulissen zu werfen und zu verstehen, für welche komplexe Systemlandschaft die Informationstechnik des Krankenhauses im Jahr 2020 steht und was sich daraus an Aufgaben ableitet.

Das Bild erinnert an den Augiasstall: Föderale Politik hemmt den Strukturwandel. Krankenhäuser sind unterfinanziert. Viele Krankenhäuser sind digital nicht vorbereitet. Sie leben mit veralteten ITK-Strukturen. Personal ohne IT-Kenntnissen, geringer Wertschätzung der Digitalisierung oder auch einem zähen Festhalten an gewohnten Betriebsabläufen.

Stichworte von Referent Thoss waren weiterhin: Mangelverwaltung, Budgetproblematik, aber besonders die Konfrontation der Beteiligten aus Verwaltung, Medizin und Pflege mit der IT. Die absurde Lage zeigte sich in vielerlei Beispielen. Eines davon ist die CheckIT-Liste des bvitg und des Marburger Bundes. Klinischen Anwendern ssoll eine handhabbare strukturierte Checkliste zur prozessorientierten Nutzenrealisierung aus eHealth Lösungen im klinischen Alltag zur Verfügung stehen. Ein weiteres Ziel ist der Kompetenzerwerb auf Seiten der Anwender in der Bewertung des Nutzenpotentials von IT im KH. Bei diesem IT-Benchmarking für die Gesundheitsversorgung waren von 48 Pflichtpunkten im Schnitt jedoch nur 4 Kriterien erfüllt.

Michael Thoss brachte es auf den Punkt: „IT macht eine schlechte Organisation nicht besser, sondern lediglich teurer. Wer ein IT-Projekt beginnt, sollte im Vorfeld immer überlegen, welche organisatorischen Änderungen neue Technologien mit sich bringen oder begünstigen. Man muss das ganzheitlich betrachten und beiden Teilen des Projektes genauso viel Aufmerksamkeit widmen."

Die digitale Transformation stellt zwangsläufig an verschiedenen Punkten der Entwicklung Ansprüche an die Unternehmensorganisation. Sie betreffen sowohl Aufbau als auch Ablauf. Wesentlich bedeutsamer sind jedoch die Rahmenbedingungen und Auswirkungen auf die Finanzierung von Dienstleistungen der IT.

Der genaue Blick auf Gesetze und Finanzierung offenbart: Es sind zwei getrennte paar Schuhe. Synergien ist dabei Fehlanzeige, sie streben in ihren Zielen sogar auseinander. In der Schlussfolgerung lässt sich sehen: Gewollt ist, dass es weniger Krankenhäuser, jedoch größere Einheiten werden. Die kleinen Häuser sollen offenbar ausgehungert werden. Blickt man dazu durch die Hintertür mit dem Kennzeichen „IK Nummer", zeigt sich eine „kalte Strukturbereinigung". Nicht alle betroffenen Kliniken können sich auf Grund der Rahmenbedingungen aus eigener Kraft erholen.

Referent Michael Thoss listete bei eHealth und der Digitalisierung brisante Hemmschwellen auf, die für den regionalen Grundversorger und sein Management nicht leicht zu überwinden sind. Im Mittelpunkt stehen Gesetzgebung, Finanzierung und auch Technologie – alle mehr oder weniger problematisch. Der regionale Grundversorger sieht in den digitalen Abgrund. Im Druckpunkt befindet sich dabei der IT-Leiter. Welche Perspektive hat er für sich? „Wenn der Geschäftsführer digitale Geschäftsmodelle verfolgt, kann es gut aussehen – andernfalls schlecht."

Referent Michael Thoss, IT-Leiter Klinikum Hochrhein, Autor und freier Berater, Mitglied im BV KH-IT

4 Netzwerke - 1 Veranstaltungsreihe

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

www.health-it-talk.de

Die engagierte Moderation übernahm Netzwerksprecher Stefan Zorn, SIBB e.V. – Verband der IT- und Internetwirtschaft Berlin/Brandenburg, imatics Software GmbH.

Aktueller Hinweis: Information Security in Healthcare Conference

Erwin Schnee, Organisator, Information Security in Healthcare Conference, hat aktuell folgenden Hinweis zur geplanten Veranstaltung am 4.6.2020 veröffentlicht:

"Wir freuen uns sehr, dass Sie sich für eine Teilnahme an der Information Security in Conference entschieden haben.
Unsere Vorfreude darauf Sie als Gast vor Ort begrüssen zu dürfen wurde aufgrund der aktuellen Lage rund um das Coronavirus abrupt getrübt. Die Gesundheit der Teilnehmer, der Referenten sowie unserer Mitarbeiter liegt uns sehr am Herzen.
Wir hoffen und gehen davon aus, dass sich die Situation in den nächsten Wochen beruhigen wird. Sollte trotz aller vom Bund ergriffenen Massnahmen die Situation länger andauern und eine Durchführung wegen Rahmenbedingungen am Donnerstag 4. Juni 2020 nicht möglich sein, würde die Konferenz auf Mittwoch 12. August 2020 verschoben. Wir beobachten die Situation aufmerksam und werden Sie auf dem Laufenden halten."

Bitte lesen Sie hierzu das Interview auf S. 70, das wir vor Ausbruch der Pandemie mit dem Organisator geführt hatten.

Kongress zu Krankenhausführung und digitale Transformation als Live-Stream

Auch in den Zeiten von Covid-19 möchte die ENTSCHEIDERFABRIK bestmögliche Leistungen in Sachen Weiterbildung und Meinungsaustausch bieten. Aufgrund der aktuellen Lage arbeiten mehr und mehr Leute im Home Office. Deshalb findet der Kongress "Krankenhausführung und digitale Transformation" vom 13.-14. Mai 2020 im digitalen Live-Stream statt. Dieser steht nicht nur den Mitgliedern der ENTSCHEIDERFABRIK zur Verfügung, sondern ist für alle Vertreter von Leistungserbringern bzw. Kliniken, Gesundheits- und Pflegedienstleistern bis auf weiteres kostenlos.

Informationen finden Sie unter
www.entscheiderfabrik.com/veranstaltungen/digitales-live-streaming-kongress

CHCIO Prüfungsvorbereitung und Prüfung

Vom 12.-14. Mai 2020 findet die Certified Healthcare CIO Zertifizierung und Prüfungsvorbereitung statt. Die eLearning Plattform für die Weiterbildung zum CHCIO (Certfied Healthcare CIO) ist nun online.

Die Kompetenzfelder bzw. Prüfungsbereiche

- Krankenhausführung und Digitalisierungsstrategie
- Technology Management
- Change Management
- Ermittlung und Management des Wertbeitrages
- Service Management
- Talent Management
- Relationship Management
- 24 Vorträge in fünf deutschsprachigen und einer englischsprachigen Session
- Beispiele für digitale Transformation aus Belgien, Deutschland, Österreich, Schweiz und USA
- Acht vertiefende Workshops von und mit Better, BEWATEC, DMI, ID - Information & Dokumentation im Gesundheitswesen, m.doc, NUANCE, RECARE und The i-engineers.

Informationen finden Sie unter
www.entscheiderfabrik.com/veranstaltungen/digitales-live-streaming-kongress

Mitgliederversammlung AHIME-Association of Health Information Management Executive

Die AHIME Vorstandssitzung und Mitgliederversammlung findet am 15. Mai statt. Die Veranstaltung wird auch als digitaler Live Stream durchgeführt. Informationen unter
www.entscheiderfabrik.com

Rückfragen beantwortet Dr. Pierre-Michael Meier, Stv. Sprecher der fördernden Verbände und Geschäftsführer der Entscheiderfabrik, unter *pierre-michael.meier@guig.org*

17 Kliniken, Gesundheits- und Pflegedienstleister profitieren

Wahl der 5 Digitalisierungsthemen der Gesundheitswirtschaft 2020

Die 5 Digitalisierungsthemen der Gesundheitswirtschaft 2020 sind gewählt – die beteiligten Kliniken können die Themen 12 Monate ausprobieren und profitieren!

Auf dem Entscheider-Event, dem sogenannten Digitalisierungsgipfel der Gesundheitswirtschaft, stellten am 12. Februar diesen Jahres die 12 Finalisten ihre Digitalisierungskonzepte vor. Auf Basis der Präsentationen wählten die anwesenden Vertreter der Krankenhaus Führungs- und Leitungsebene die "5 Digitalisierungsthemen der Gesundheitswirtschaft", die im Jahr 2020 von Industrie, Beratern und Krankenhäusern bearbeitet werden.

Für den Entscheider-Event 2020 hatten sich im Düsseldorfer Industrieclub 644 Akteure aus der Krankenhaus Unternehmens-, Informationstechnik-und Medizintechnikführung angemeldet. Seit 2006 hat der IuiG-Initiativ-Rat, in dem die 36 fördernden Verbände der ENTSCHEIDERFABRIK vertreten sind, das Format des Entscheider-Zyklus aus Entscheider-Event, Sommer-Camp und Ergebnis-Veranstaltung (GDK / MEDICA) stetig weiter verbessert und erweitert.

Die 5 Digitalisierungsthemen 2020 sind:

Archivar4.0 - der Chief Data Officer als Berater der Krankenhausführung für Nutzen stiftende Services-Apps auf Basis des hauseigenen

Entlastung der Pflegefachkräfte und ökonomische Steuerung mittels einer prädiktiven Pflege-Controlling-Unit

MIA ROBOTIC CODING, Die Digitalisierung der Kodierung – Erlössteigerung aus Big Data

Arbeite doch einfach wann Du willst!" Zufriedene Mitarbeiter durch Selbstplanung auf Basis einer Jahreskapazitätsplanung

Lückenlose digitale Unterstützung bei der Schlaganfallversorgung – mittels Vernetzung aller Akteure und KI-Bildanalyse zur optimalen Therapie

Insgesamt wählten sich 17 Krankenhäuser auf die 5 Digitalisierungsthemen der Gesundheitswirtschaft und beteiligen sich somit an diesen, d.h. die Kliniken können diese Digitalisierungsprojekte nun 12 Monate auf ihren Nutzen kostenfrei testen und vermeiden somit Fehlinvestitionen.

Die ENTSCHEIDERFABRIK bietet daher ein sehr interessantes einmaliges Veranstaltungsformat, das an den folgenden Mehrwerten orientiert ist:

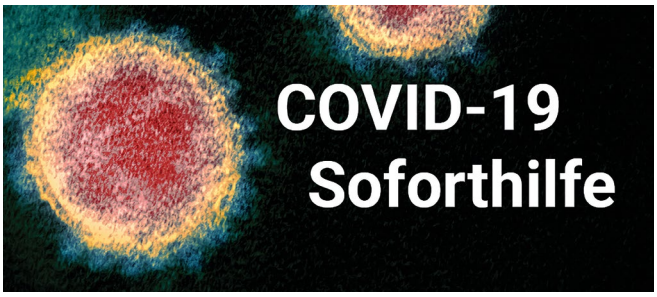
- Wirtschaftlichkeit der Krankenhäuser
- Verbesserung der Behandlungsqualität der Patienten

Während der Veranstaltung wurde auch die Düsseldorfer Erklärung beschlossen. Diese richtet sich in drei konkreten Forderungen in einem eindringlichen Appell an die politischen Entscheidungsträger auf Landes- und Bundesebene: "Wir befinden uns im Schraubstock. Zu Recht erwarten die Menschen von uns, dass wir ihnen in jeder medizinischen Notlage bestmöglich helfen. Diesen Auftrag nehmen wir auch unter schwierigen Rahmenbedingungen an. Aber, die Politik macht es den Krankenhäusern derzeit immer schwerer – zum Teil sogar unmöglich – ihre Aufgaben zu erfüllen. Immer neue Lasten werden uns aufgebürdet, völlig unnötige Bürokratie halten Ärzte und Pflegende von ihrer eigentlichen Arbeit ab. Der Staat erfüllt seit Jahren seine gesetzlich vorgeschriebene Pflicht dagegen nicht.", heißt es in der Erklärung.

Weitere Informationen unter **www.Entscheiderfabrik.com**

Agfa HealthCare erweitert bestehende Lösungen um spezifische Funktionalitäten

Soforthilfe für ORBIS-Kunden in *Corona-Zeiten*



#zusammenhalten #WirSindFürSieDa: Mit diesen Hashtags überschreibt Agfa HealthCare sein Paket an Soforthilfen, mit denen der Anbieter ORBIS-Anwender kurzfristig bei der Bewältigung der zusätzlichen und neuartigen Herausforderungen rund um das Coronavirus SARS-CoV-2 unterstützt. Zu dieser Soforthilfe gehören neue Protokolle und Dokumentationen, die für Krankenhäuser im Zuge der COVID-Pandemie eine schnelle Abbildung, Erfassung und Auswertung möglich machen. So entstehen immer wieder neue Lösungen. Ein wesentliches Ziel der einzelnen Lösungen ist es, die Informationen zur Infektiosität einzelner Patienten sichtbar zu machen.

Unterstützung für Intensivstationen

Gerade für die Intensivstationen in Kliniken steigen die Belastungen durch SARS-CoV-2 an. Alle Einrichtungen, die den ORBIS ICU-Manager nutzen, werden von Agfa HealthCare unterstützt.

Diese Krankenhäuser erhalten auf Nachfrage zeitlich begrenzt bis zum 30. September 2020 kostenfreie Bettlizenzen, um den erhöhten Dokumentationsbedarf durch die zusätzlichen Betten und die erwartet höheren Behandlungszahlen abzudecken.

Update für ORBIS Infektionsmanagement

Für ORBIS Infektionsmanagement und ORBIS Hygiene-Monitor hat Agfa HealthCare den Erregerkatalog um SARS-CoV-2 erweitert und ermöglicht so eine differenzierte Dokumentation und Auswertung von Infektionsfällen sowie deren grafische Darstellung.

Zudem gibt es einen expliziten Meldebogen für COVID-19-Fälle gemäß §6 IfSG, der sowohl für die interne Dokumentation als auch für die Meldung von Verdachts- und laborbestätigten Fällen genutzt werden kann. Auch besteht die Möglichkeit, den bereits verwendeten Meldebogen nach §§6,8,9 IfSG um COVID-19 zu erweitern. Mit diesen Maßnahmen wird den Gesundheitseinrichtungen die Meldung von Corona-Patienten erheblich vereinfacht.

Für Kunden, die die entsprechenden Programme einsetzen, ist das Update kostenfrei.

ORBIS AddOn Verdachtsdokumentation COVID-19

Das ORBIS AddOn Verdachtsdokumentation COVID-19 ist eine Soforthilfe für Gesundheitseinrichtungen, die ORBIS Infektionsmanagement aktuell nicht einsetzen. Agfa HealthCare stellt diesen ORBIS-Kunden die Lösung lizenz- und wartungskostenfrei zur Verfügung.

Das AddOn Verdachtsdokumentation COVID-19 beinhaltet ein Dokumentationsformular für Verdachtsfälle, das über ein Kontextmenü aufgerufen werden kann. Es ermöglicht die Dokumentation von COVID-19-Verdachtsfällen sowie der relevanten Symptom-, Test- und Meldungsinformationen anhand der Kriterien des Robert-Koch-Instituts (RKI). In einer

Kostenfreie Bettlizenzen für den ORBIS ICU-Manager, um den erhöhten Dokumentationsbedarf zu bewältigen.

Arbeits- und Prüfliste, die individuell gefiltert werden kann, werden alle dokumentierten Fälle, offenen Testergebnisse und offenen Meldungen beim Gesundheitsamt dargestellt. Im nächsten Schritt können dann alle Informationen zu durchgeführten Tests und der Infektiosität einzelner Patienten sowohl in die Arbeitsliste Triage wie auch in die Raumbelegungsübersicht und die Notfallakte übernommen werden. Weiterhin ist der CRB-65, also der klinische Score, mit dem der Schweregrad einer ambulant erworbenen Pneumonie abgeschätzt werden kann, als relevantes Assessment umgesetzt. Nicht zuletzt können im AddOn Verdachtsdokumentation COVID-19-Kontaktpersonen dokumentiert werden.

Differenzierte Dokumentation und Auswertung von Infektionsfällen mit einem erweiterten Erregerkatalog.

Unterstützung bei der Bettensuche und -belegung

Mit dem ORBIS AddOn Bettensuche/Belegungsübersicht steht den ORBIS-Kunden im Rahmen der COVID-19-Soforthilfe ein weiteres Tool zur Verfügung – ohne Lizenz- und Wartungskosten bis zum 31. Dezember 2020.

Die Belegungsübersicht ermöglicht den Anwendern einen einfachen und schnellen Überblick über die Belegungssituation auf den Stationen. Dabei lenken Filterprofile den Blick auf die relevanten Informationen. Separat ausgewiesen sind dabei COVID-19-(Verdachts-)Fälle sowie Raum- und Bettsperren. Für den Umgang mit Beatmungsplätzen wurde das AddOn kurzfristig um eine Liste der beatmeten Patienten ergänzt, die auch die Kapazitätsauslastung anhand einer definierten Belastungsgrenze (Beatmungsmaschinen) ausweist.

Für die Bettensuche ermöglicht das AddOn einen schnellen Überblick über die gesamte Auslastung des Hauses auf Stationsebene sowie eine Darstellung der Stationsauslastung in Tabellenform. Freie Betten können dann allgemein und im Patientenkontext gesucht werden. Auch ein direkter Aufruf des Verlegungsdialogs oder der Fallkorrekturen sind möglich. Dabei werden zahlreiche Kennzahlen, etwa geplante Aufnahmen und Entlassungen, berücksichtigt.

Vereinfachte Dokumentation und Meldung von COVID-19-(Verdachts-)Fällen.

Dienstleistungsangebote

Für den Umgang mit COVID-19-(Verdachts-)Fällen müssen die Gesundheitseinrichtungen neu denken – es gibt eine Blaupause. Sicher ist, dass die Strukturen und Arbeitsweisen angepasst werden müssen. ORBIS kann auf diese Anforderungen vorbereitet und entsprechend konfiguriert werden.

Damit sich die Mitarbeiter in den Kliniken ganz der Patientenversorgung widmen können, unterstützt Agfa HealthCare seine Kunden bei individuellen Anpassungen der vorhandenen Software. Dazu haben die Systemexperten den zeitlichen Mindestaufwand für die Implementierung der „Standardeinrichtung" ermittelt und bieten den Kunden kleine Dienstleistungspakete zu weiteren Ergänzungen im Rahmen der COVID-19-Pandemie an.

Viele Kliniken richten beispielsweise Erstsichtungszentren auf Basis des Cockpits Notaufnahme als zusätzliche Einheit der Zentralen Notaufnahme ein. Diese Implementierung ist nicht trivial und kann durch Agfa HealthCare zeitnah unterstützt werden.

Als weitere Dienstleistungspauschalpakete können ORBIS-Kunden die Implementierung der COVID-19-Verdachtsdokumentation, die Aktualisierung des Cockpits Notaufnahme sowie die befristete Inbetriebnahme des AddOns Bettensuche/Belegungsübersicht in Anspruch nehmen.

Weitere Informationen und Updates finden Interessierte auf der Website **www.agfahealthcare.de**.

Schnelle Bettenübersicht und -belegung unter besonderer Berücksichtigung infektiöser Patienten.

Lahn-Dill-Kliniken, Standort Wetzlar

Risikomanagement der Krankenhaus-IT im Zeichen von KRITIS

Krankenhäuser zählen aufgrund ihrer herausragenden Bedeutung für das Wohlergehen und den Schutz der Bevölkerung zu den Kritischen Infrastrukturen unserer Gesellschaft. Sie haben daher eine besondere Verpflichtung, die Verfügbarkeit ihrer Dienste und der Prozesse, mit denen diese erbracht werden, sicherzustellen.

Die Vernetzung der Office-IT und der Medizintechnik (übergreifende Patientendaten), mobile Arbeitsplätze, Digitalisierung und der Mangel an Fachpersonal sind eine besondere Herausforderung für die Krankenhaus-IT. Damit einher entstehen neue Verwundbarkeiten und Risiken. Damit es aufgrund eines IT-Ausfalls nicht etwa zu Reputationsschäden der Einrichtung, finanziellen Verlusten oder gar im schlimmsten Fall zu einer Gefährdung von Leib und Leben der Patienten kommt, sind die Herausforderungen durch die IT-Nutzung in das übergreifende Risikomanagement zu integrieren.

Bisher konnte das Management der Krankenhaus-IT jeder für sich allein nur auf einen Leitfaden „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT“ zurückgreifen und methodisch (RiKrIT) im Sinne der Kritikalität (Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Daten) technische und/oder organisatorische Maßnahmen entwickeln.

Im Oktober 2019 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus anerkannt. Das B3S Papier dient der Etablierung eines angemessenen Sicherheitsniveaus i. S.v. § 8a (1) BSIG bei gleichzeitiger Wahrung des üblichen Versorgungsniveaus der Patientenversorgung und der Verhältnismäßigkeit der umzusetzenden Maßnahmen nach heutigem Stand der Technik.

In das B3S Papier sind viele bestehende Standards (ITIL, ISO 27001, BSI IT-Grundschutz, …) und Anforderungen aus der Regulatorik (BSIG, DSGVO, BDSG, …) eingeflossen und damit ein klares Muss für Krankenhäuser, die heute schon unter KRITIS fallen. Für die Krankenhäuser aber, die noch nicht KRITIS sind, ist das Papier ein hervorragender Leitfaden für die Umsetzung eines Minimums an IT-Sicherheit.

Um nicht die nächsten Jahre die Zeit mit reiner Konzeptarbeit zu vergeuden, empfehlen wir:

Das Klinikum Wetzlar ist auf KRITS 2.0 vorbereitet

- Die Einführung eines ISMS, welches die Anforderungen des B3S-Standards umsetzt
- die Protokollierung (B3S, Kapitel 7.3.15) zuerst zu starten (als Basis für die Umsetzung vieler technischer und organisatorischer Maßnahmen bei der Einführung eines ISM – System in der Krankenhaus IT)
- Die Erstellung eines Protokollierungs- und Auswertungskonzeptes (RiKrIT) mit Definition eines Rollenkonzeptes, N-Augen-Prinzip für die Depseudonymisierung, Art und Umfang der Protokollierung. Zielpersonen des Konzeptes sind Auditoren, Revisoren und Datenschützer
- Zur Erfüllung der Vorgaben aus der DSGVO wurde der Appliance-Gedanke umgesetzt und mit dokumentierten TOMs sichergestellt, dass kein IT-Admin gewollt oder ungewollt gegen Datenschutz verstoßen kann
- Gemäß BDSG § 76 Protokollierung werden innerhalb des Log-Management-Systemes sämtliche Aktionen mit einer Zweckbindung versehen und protokolliert
- Die Standardbericht- und Alarmierungspakete dienen dem auditsicheren Nachweis der Kontrolle und sind Bestandteil der Softwarewartung (keine Folgekosten)

Die Lahn-Dill-Kliniken sind bereits in der Umsetzung und bereiten sich auf KRITIS 2.0 vor.

Folkert Hoim, Leiter IT der Lahn-Dill-Kliniken: „Wir waren auf der Suche nach einem Werkzeug für die Protokollierung, das einfach zu managen, nicht komplex und nicht teuer ist, um die Anforderungen zu erfüllen, die an kritische Infrastrukturen gestellt werden."

Thilo Berger, stellvertretender IT-Leiter und Bereichsleiter Netzwerk- und Systembetrieb: „Gemeinsam mit der NETZWERK Software GmbH haben wir die Log-Management-Lösung ProLog umgesetzt. Dank dem Einsatz von bestehenden Standards konnte in kürzester Zeit das Protokollierungskonzept erstellt, die technische Integration der ProLog-Appliance und die Anbindung der vielen unterschiedlichen Quellen umgesetzt werden. Die umfangreichen Auswertungsmöglichkeiten haben bereits auf den ersten Blick beeindruckt."

Michael Wiesner, externer Informationssicherheitsbeauftragter bei den Lahn-Dill-Kliniken freut sich über die schnellen Resultate: „Wir haben im Informationssicherheitsmanagement (ISMS) und aus dem B3S-Standard vielfältige Anforderungen an das Log-Management, deren Überwachung mir obliegt. Bereits kurze Zeit nach der Inbetriebnahme der Lösung konnten aussagekräftige Berichte erzeugt werden, die mir die Erfüllung meiner Aufgaben immens erleichtern."

Die eigentlichen Treiber für den Einsatz eines zentralen Log-Management System wie ProLog sind die Erhöhung der IT-Sicherheit und der IT-Verfügbarkeit dank der vollen Transparenz über die IT-Events, die Möglichkeit der Alarmierung in Echtzeit und der forensischen Suche. Aber erst die Kombination der kompletten ProLog-Lösung aus Protokollierungskonzept, SW-Werkzeug, fertigen Berichts- und Alarmierungspakete, Umsetzung der DSGVO und BDSG Vorgaben macht die Krankenhaus-IT auditsicher im Sinne von B3S oder einer ISO27001-Zertifizierung. Alle Details über ProLog finden Sie unter www.prosoft.de/prolog.

Autor: Olaf Müller-Haberland,
Co-Founder (www.NETZWERK.de)

Folkert Hoim, Leiter IT der Lahn-Dill-Kliniken

HEIDELBERG EYE EXPLORER

Digitale Trendwende in der *Augenheilkunde*

Die Digitalisierung bietet viele Vorteile, die jede Augenklinik zu Workflow-Optimierungen und Datensicherheit sowie im Sinne des Patienten nutzen sollte. Wichtige Ansätze sind zum Beispiel ein robustes Bilddatenmanagement-System, die Integration diagnostischer Geräte oder eine speziell für die Augenheilkunde entwickelte elektronische Patientenakte. Dies kann kostbare Zeit einsparen und typische Fehler im Datenmanagement vermeiden.

Die Berührungspunkte von Augenärzten mit dem Thema Digitalisierung sind bislang noch sehr unterschiedlich. Während manche in ihrer Forschung sich schon aktiv mit künstlicher Intelligenz und Big Data beschäftigen, stehen andere den digitalen Hilfsmitteln noch zögerlich gegenüber. Als etablierter Hersteller von diagnostischen Geräten hat Heidelberg Engineering den Bedarf an digitalen Lösungen im Bereich der Augenheilkunde bereits vor einigen Jahren erkannt und seitdem in deren Entwicklung investiert, um so Augenärzte bei der optimalen Patientenversorgung zu unterstützen.

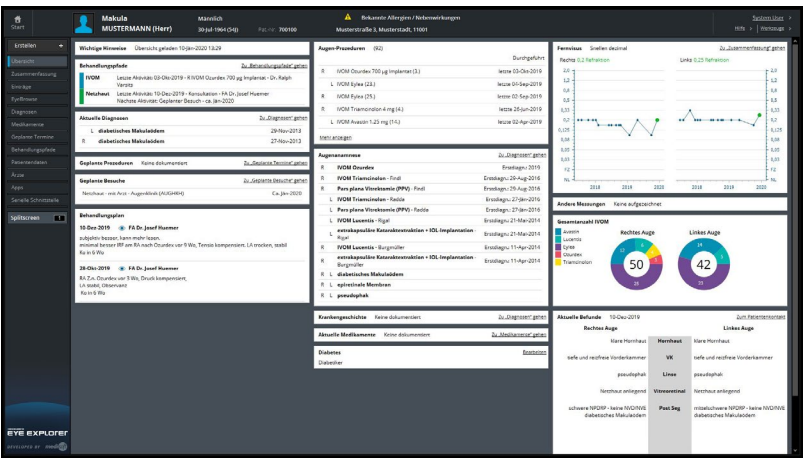
Heidelberg Engineering bietet mit der HEIDELBERG EYE EXPLORER Produktpalette IT-Lösungen zur Optimierung digitaler Prozesse in der Augenheilkunde an. Um präzise klinische Entscheidungen effizient treffen zu können, ist ein schneller Zugang zu allen relevanten klinischen Informationen notwendig. Multimodale Diagnostik erlaubt es, Untersuchungsdaten und -bilder unterschiedlicher Bildgebungsmodalitäten auf einen Blick zu betrachten. Da bei den meisten Pathologien der Krankheitsverlauf entscheidend für das weitere Therapiemanagement ist, spielen regelmäßige Verlaufskontrollen eine wichtige Rolle. Dafür müssen alle erhobenen Daten über einen längeren Zeitraum hinweg gespeichert werden. Die Kombination aus relevanten Diagnose- und Bilddaten mit therapeutischen Informationen in einer zentralen Patientenakte ermöglicht den vollen Blick auf den Patienten, was zu einem verbesserten Therapiemanagement durch einfachere Arbeitsprozesse beiträgt.

Alle IT-Lösungen der HEIDELBERG EYE EXPLORER Produktfamilie sind für die Augenheilkunde optimiert, modular kombinierbar und können individuell je nach Praxis- oder Klinik-Anforderungen skaliert werden. Mit HEYEX 2, HEYEX PACS und HEYEX EMR stellen Sie Ihre augenärztliche Praxis oder Klinik optimal für die Zukunft auf.

- **HEYEX 2** ist die Bilddatenmanagement-Lösung, die Ihnen einen schnellen und einfachen Zugriff auf diagnostische Aufnahmen, Berichte und Karten von all Ihren Heidelberg Engineering Geräten gewährt und Sie so bei einer effizienten Diagnostik unterstützt.. Die Aufnahme, Verwaltung und Bewertung sowie die Speicherung und Archivierung diagnostischer Bilder ist in einer einzigen Plattform möglich.

- **HEYEX PACS** ist die Integrationslösung, die Ihnen die Anbindung der Heidelberg Engineering Produktpalette an Informationsquellen von Fremdanbietern ermöglicht. Optimieren Sie Ihre Arbeitsabläufe, indem Sie doppelte Datenhaltung vermeiden und geltende Standards besser einhalten.

- **HEYEX EMR** *(Abbildung unten)* ist die Lösung für elektronische Patientenakten, die Ihnen eine flexible und intuitive Benutzeroberfläche für ophthalmologische Patientendaten bietet. Umfassende Dokumentationsmöglichkeiten unterstützten Sie dabei, qualitativ hochwertige Patientendaten strukturiert zu erfassen und gleichzeitig Ihre Klinik-Ressourcen effizient einzusetzen.



HEYEX EMR zeigt alle relevanten Patienteninformationen, wie z.B. Krankengeschichte, Therapien oder Entwicklung des Sehvermögens.

Fazit

Für Heidelberg Engineering stellen die optimierte Bildverwaltung und Geräteintegration sowie eine strukturierte elektronische Patientenakte schon heute wichtige Säulen für die Augenklinik von morgen dar. Mit den modularen HEIDELBERG EYE EXPLORER Software-Lösungen kann die Effizienz in ausgelasteten Augenkliniken gesteigert und die Patientenversorgung nachhaltig verbessert werden.

Mehr Informationen unter *www. heidelberg-eye-explorer.com*

Kundenstimmen

Peter Mussinghoff, Geschäftsführer des Augenzentrums am St. Franziskus-Hospital, Münster

„Um auch in Zukunft die vielfältigen Möglichkeiten der Bildgebung effizient und im Sinne der Patienten einsetzen zu können, ist es jetzt an der Zeit, auch in der Ophthalmologie leistungsfähige Systeme zu etablieren, die diesen Anforderungen gewachsen sind.“

Dr. Stefan Bültmann, Augenarztpraxis Bültmann, Ladenburg

„Bei uns in der Augenheilkunde werden immer größere Mengen an visuellen Daten erzeugt. Mit den wachsenden Bilddatenmengen braucht man eine gute Verwaltungsoberfläche um Daten schnell wiederzufinden. Mit HEYEX 2 habe ich jetzt eine technisch solide Plattform, die es mir ermöglicht Aufnahmen parallel darzustellen, auszuwerten und zu befunden. Mit HEYEX 2 kann ich sogar fremde Bilder von anderen Geräten über die Viewer-Funktion integrieren und mit in die Differenzialdiagnostik einbeziehen. […] Ich entdecke immer noch neue Stärken und Möglichkeiten für meinen Praxisalltag.“

Wo gibt es freie Intensivbetten für COVID-19-Erkrankte?

Das Robert Koch-Institut (RKI) und die Deutsche Interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin (DIVI e. V.) haben gemeinsam mit SAS eine Informations- und Prognoseplattform aufgebaut, die einen Überblick über den Bestand und Bedarf an freien Intensivbetten mit Beatmungsgeräten gibt. SAS, einer der weltweit führenden Anbieter von Analytics-Lösungen, hat diese Plattform als Partner des RKI innerhalb weniger Tage realisiert.

Mit dem Einsatz von SAS Software schafft das neue Informationssystem in Echtzeit Transparenz bezüglich der Belegung der vorhandenen Intensivbetten und erlaubt Vorhersagen zu den benötigten Kapazitäten. Behörden und Kliniken können ihre Ressourcenverteilung sogar schon im Vorfeld dem zu erwartenden Bedarf anpassen. Zudem stehen interaktive Berichte zum Lagebild für die bessere Planung der Einsatzkräfte und -mittel bereit.

Auf diese Weise kann analytische Software helfen, eine der größten Herausforderungen im Verlauf einer Pandemie wie durch SARS-CoV-2 zu lösen: intensivmedizinisches Personal und Ressourcen evidenzbasiert so zu koordinieren, dass sie genau dort zur Verfügung stehen, wo und vor allem wann sie gebraucht werden.

SAS wurde bei der Umsetzung des Projektes von der PRODYNA SE unterstützt, einem der europaweit führenden Softwarehäuser für Individualentwicklung in der Cloud.

„Bei der Ausbreitung einer Pandemie ist vor allem Tempo gefragt. Das Analyseprojekt mit dem RKI haben wir innerhalb weniger Tage aufgesetzt", erklärt Andreas Effinger, Projektverantwortlicher und Experte für das Thema Healthcare bei SAS in Deutschland, Österreich und der Schweiz. „Und das ist erst der Anfang. Eine solche zentrale Plattform ist die Basis, um auch über die Pandemie hinaus anhand von Daten in die Zukunft zu schauen, klinikübergreifend zusammenzuarbeiten – und damit das Gesundheitswesen ein Stück weit zu revolutionieren."

Über Grenzen hinweg

Und ein solches Projekt hat auch Potenzial über Ländergrenzen hinweg. „Das Projekt mit dem RKI und dem DIVI könnte sehr gut als Blaupause für andere Länder dienen, um die Versorgung der Schwerkranken in der Pandemie zu sichern. Es müssen jetzt alle an einem analytischen Strang ziehen, auch über Ländergrenzen hinweg", meint Effinger.

SAS verfügt über Erfahrung im Bereich Healthcare-Lösungen und kann bereits auf zahlreiche ähnliche Initiativen in der Vergangenheit zurückblicken.

Forsa/SAS

Optimierte Patientenversorgung, bessere Therapieergebnisse

Analytics von SAS schafft in unterschiedlichsten Bereichen des Gesundheitswesens Mehrwerte. Moderne Technologien wie künstliche Intelligenz (KI), Bilderkennung und Machine Learning können automatisiert Aufgaben übernehmen und beispielsweise die Erstellung präziser Diagnosen erheblich beschleunigen. Mit umfassender Branchenexpertise und Healthcare Analytics hilft SAS Klinken und anderen medizinischen Einrichtungen dabei, bessere Entscheidungen zu treffen und Ressourcen effizienter einzusetzen. SAS stellt dafür unter anderem Lösungen für Kostenanalyse, Personalplanung und Performance Management sowie Advanced Analytics und KI-Ansätze bereit.

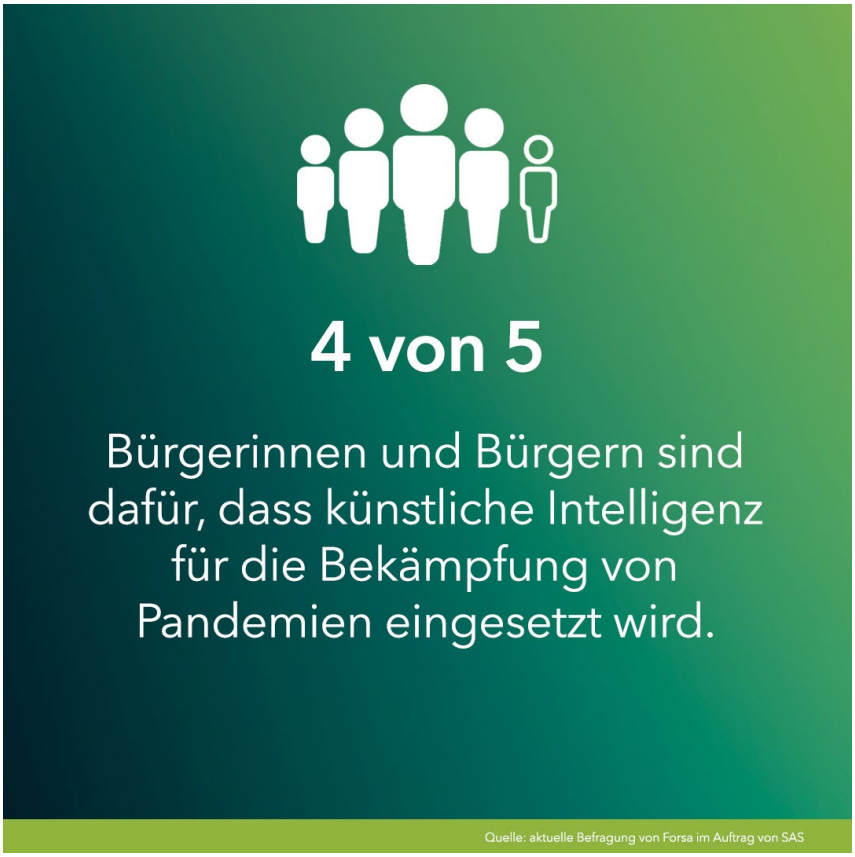
KI bringt Mehrwert im Gesundheitswesen

Welchen Stellenwert KI im Gesundheitswesen spielt, zeigt auch eine aktuelle Forsa-Umfrage, die SAS in Auftrag gegeben hat. Tendenz: Die Befragten sehen den Nutzen von KI – auch und vor allem in der Gesundheitsversorgung. Und sie wären mehrheitlich bereit, ihre Daten zur Verfügung zu stellen, wenn dadurch Pandemien eingedämmt werden können (siehe Infografiken). Befragt wurden rund 1.000 Bundesbürger ab 18 Jahren.

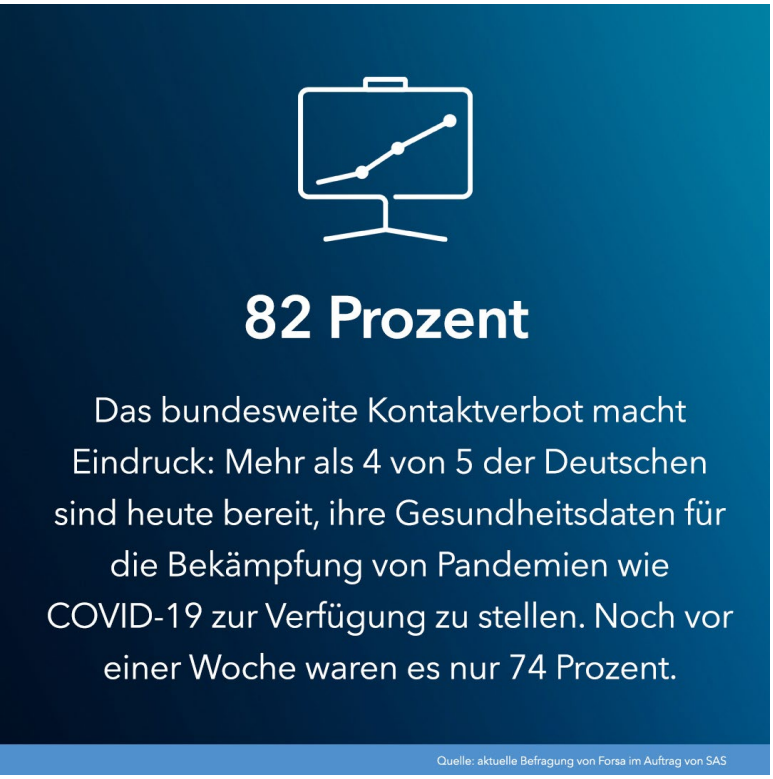
„Im Gesundheitswesen können Analytics und KI Berge versetzen – wenn man sie lässt", so Effinger. „Wir von SAS helfen beispielsweise sehr effektiv bei der Krebsfrüherkennung, bei der Reduzierung von Sepsisfällen in Krankenhäusern oder Medikamentenmissbrauch – auch dank jahrzehntelanger Erfahrung."

SAS arbeitet aktuell in 49 Ländern mit rund 1.300 Kunden aus dem Bereich Healthcare zusammen.

Weitere Informationen gibt es unter: **www.sas.com/de_de/industry/health-care.html.**



Forsa/SAS



Forsa/SAS

Über SAS

SAS ist ein führender Anbieter von Lösungen für künstliche Intelligenz (KI) und Analytics. Der Softwarehersteller spielt eine wichtige Rolle für die Digitalisierung von Unternehmen, die strategische Entscheidungsprozesse auf Datenbasis optimieren und operative Vorgänge automatisieren wollen. Aktuell setzen Unternehmen in 147 Ländern und an rund 83.000 Standorten Lösungen von SAS ein – darunter 92 der Top-100-Unternehmen im Fortune-500-Index, von Allianz bis Volvo und von Fraport bis Nestlé.

SAS hat seinen Hauptsitz in Cary, NC (USA). Die Zentrale für die Region DACH befindet sich in Heidelberg. In Deutschland betreibt SAS fünf weitere Standorte. Die Niederlassungen für die Schweiz und Österreich befinden sich in Wallisellen bei Zürich und in Wien.

Bereits 1976 gegründet, verfügt SAS über die branchenweit größte Erfahrung im Einsatz von Advanced und Predictive Analytics, Machine Learning, Cloud und IoT Analytics. Dabei kann SAS die gesamte analytische Wertschöpfungskette vom Datenmanagement bis hin zu Forecasting und Prozessoptimierung übernehmen. Heute bietet das Unternehmen eine vollständige und modulare Palette von Software und Services an, die je nach Bedarf als Managed Services in der Cloud oder beim Unternehmen vor Ort laufen. SAS bietet KI und Analytics zudem auch als reine Dienstleistung (Results as a Service).

Kostenloses Angebot von Zerto während Covid-19

Träger in der Gesundheitsbranche und der Öffentlichen Verwaltung können die IT-Resilienz-Plattform Zerto bis Ende September 2020 kostenlos nutzen, um die Verfügbarkeit ihrer Dienste zu garantieren.

Der Coronavirus bringt das Gesundheitswesen an die Grenzen seiner Belastbarkeit. Nicht nur Ärzte und Pflegekräfte sind voll eingespannt, auch die Verwaltung und die IT der Träger stehen vielerorts unter immensem Druck. Ein Ausfall der IT, beispielsweise durch einen erfolgreichen Ransomware-Angriff oder einen Hardwareausfall, würde Krankenhäuser im derzeitigen Corona-Ausnahmezustand natürlich vor immense Probleme stellen. Um die IT betroffener Organisationen in der aktuellen Situation aktiv zu unterstützen, bietet Zerto seine marktführende IT-Resilienz-Plattform ab sofort bis Ende September 2020 kostenlos zur Verfügung.

Eine IT-Resilienz-Plattform erhöht die Widerstandsfähigkeit der IT

IT-Resilienz-Plattformen sind derzeit der Goldstandard IT-Systeme vor Ausfällen jeder Art zu schützen. Die innovativen Software-Lösungen nutzen Continuous Data Protection (CDP) mit Journaling um Dienste im Notfall sofort per Mausklick wiederherstellen zu können. So können IT-Abteilungen die Verfügbarkeit ihrer Dienste jederzeit garantieren. Krankenhäuser sind seit Jahren beispielsweise beliebte Ziele für Ransomware-Attacken und die Cyberkriminellen nutzen die Zwangslage von Krankenhäusern schamlos aus, um Lösegeld zu erpressen. Mit der Nutzung einer IT-Resilienz-Plattform erhöhen Organisationen das Niveau der Widerstandsfähigkeit ihrer IT um ein Vielfaches und helfen somit dabei die Krise besser zu bewältigen.

Zerto - Marktführer in Sachen IT-Resilienz

Zerto ist ein 2009 gegründeter Technologieanbieter aus Boston und Israel, der Zerto IT Resilience Platform, Software für Disaster Recovery, Backup und Workload-Mobilität für virtualisierte Infrastrukturen und Cloud-Umgebungen anbietet. Zerto's Softwareplattform bietet kontinuierliche Verfügbarkeit, um Anwendungen zu schützen, wiederherzustellen und frei über Hybrid- und Multi-Clouds zu bewegen. Zerto genießt weltweit das Vertrauen von über 7.000 Kunden, kooperiert mit mehr als 1.100 Partnern und stellt die Basis für die Resilienz-Angebote für über 350 Cloud-Service-Provider.

Zerto während Covid-19 kostenlos nutzen

Organisationen in der Gesundheitsfürsorge oder andere systemkritische Dienste, die Verwaltungen von Bund, Ländern und Kommunen und andere Organisationen, die während der COVID-19-Pandemie direkt Unterstützung für die Gemeinschaft leisten, erhalten:

- Kostenlose Zerto-Lizenzen für den Schutz von bis zu 50 virtuellen Maschinen bis zum 30.9.2020
- Kostenlosen Premium-Support
- Unterstützung bei der Installation und Online-Schulung
- Kostenfreie Nutzung von Zertos "Educational Labs".

Technische Voraussetzungen

Zerto sichert virtualisierte Dienste auf VMware vSphere oder Microsoft HvperV basierenden Umgebungen ab. Die Software ist sehr einfach zu konfigurieren und zu nutzen.

Um die kostenlosen Lizenzen für Zerto zu erhalten, registrieren Sie sich bitte hier:
www.zerto.com/page/zerto-free-offer-for-healthcare-and-government-organizations/

Dr. Aykut M. Uslu, USLU MEDIZININFORMATIK, Düsseldorf

Beschaffung von Medizinprodukten in Zeiten von Corona-Pandemie

Die Beschaffung von Medizinprodukten durch kommunale Krankenhäuser mit ihren Bindungen an vergaberechtliche Regelungen vollzieht sich unter normalen Umständen in geordneten Bahnen über Einkaufsverbünde oder Selbstbeschaffung. Die Bewältigung einer Pandemie wie die derzeitige Corona-Pandemie stellt dieses System vor Herausforderungen. Wie können in diesen Zeiten Medizinprodukte strukturiert beschafft werden?

Ausgangslage

Ende Dezember ist erstmals in China der Virus mit der Bezeichnung SARS-CoV-2 (Severe Acute Respiratory Syndrome Coronavirus 2, „Schweres akutes Atemwegssyndrom Coronavirus 2"; vormals 2019-nCoV) aufgetreten. Das Bundesgesundheitsministerium beschafft inzwischen Schutzkleidung für Ärzte und medizinisches Personal zur Behandlung von Covid-19-Patienten, und zwar verstärkt aus deutscher Herstellung. Auf der Homepage des Ministeriums finden sich Vergabeunterlagen zum Abschluss entsprechender Rahmenverträge für in Deutschland gefertigte persönliche Schutzausrüstung wie Atemmasken, OP-Masken oder Schutzkittel (https://www.bundesgesundheitsministerium.de/ministerium/meldungen/2020/herstellung-schutzausruestung.html).

Die Versorgung mit Schutzmasken und Schutzkleidung in Deutschland soll dadurch unabhängiger vom Weltmarkt werden. Die Abnahmegarantie der Verträge soll für Unternehmen ein Anreiz sein, eine Produktion aufzubauen.

Schritte zur Basishygiene

Es empfiehlt sich nunmehr eine konsequente Umsetzung der Basishygiene einschließlich der Händehygiene in allen Bereichen des Gesundheitswesens. Ein mehrlagiger medizinischer Mund-Nasen-Schutz (MNS) ist geeignet, die Freisetzung erregerhaltiger Tröpfchen aus dem Nasen-Rachen-Raum des Trägers zu behindern und dient primär dem Schutz des Gegenübers (Fremdschutz). Gleichzeitig kann er den Träger vor der Aufnahme von Tröpfchen oder Spritzern über Mund oder Nase, z. B. aus dem Nasen-Rachen-Raum des Gegenübers, schützen (Eigenschutz). Aufgrund dieser Eigenschaften wird das generelle Tragen von MNS durch sämtliches klinisches Personal mit direktem Kontakt zu besonders vulnerablen Personengruppen auch außerhalb der direkten Versorgung von Sars-CoV-2-Patienten aus Gründen des Patientenschutzes während der Pandemie empfohlen.

Durch das korrekte Tragen von MNS innerhalb der medizinischen Einrichtungen kann das Übertragungsrisiko auf Patienten und anderes medizinisches Personal bei einem Kontakt von <1,5 m reduziert werden. Atemschutzmasken mit Ausa-

temventil sind nicht zum Drittschutz geeignet. Als ergänzende Maßnahmen im klinischen Bereich wird die Einzelunterbringung in einem Isolierzimmer mit eigener Nasszelle empfohlen. Die Nutzung eines Isolierzimmers mit Schleuse/Vorraum ist grundsätzlich zu bevorzugen; eine gemeinsame Isolierung mehrerer Patienten ist unter bestimmten Bedingungen möglich.

Risiken durch raumlufttechnische Anlagen, durch die eine Verbreitung des Erregers in Aerosolen auf andere Räume möglich ist, sind vor Ort zu bewerten und zu miniminieren.

Zur persönlichen Schutzausrüstung wird der Einsatz geschulten Personals für die Versorgung von Sars-CoV-2-Patienten welches möglichst von der Versorgung anderer Patienten freigestellt wird, empfohlen.

Bei Einhaltung der Technischen Regeln kann der Arbeitgeber insoweit davon ausgehen, dass die entsprechenden Anforderungen der Verordnung erfüllt sind. Wählt der Arbeitgeber eine andere Lösung, muss er damit mindestens die gleiche Sicherheit und den gleichen Gesundheitsschutz für die Beschäftigten erreichen spezifiziert.

Eine Händedesinfektion mit einem Desinfektionsmittel mit nachgewiesener, mindestens begrenzt viruzider Wirksamkeit nach Ausziehen der Handschuhe und vor Verlassen des Zimmers ist notwendig.

Beschaffung von Medizinprodukte (Geräte)

Als Medizinprodukte gelten alle Apparate, Instrumente, Vorrichtungen, aber auch Software und Stoffe, die für die Diagnose, Therapie oder Prävention von Krankheiten beim Menschen vorgesehen und keine Arznei- oder Lebensmittel sind. Typische Medizinprodukte stellen dar: Pflegebetten, Verbandmittel, Ultraschallgeräte, Herzkatheter.

Neben Mobiliar für Krankenzimmer (Betten, Schränke) sind auch medizinische Geräte wie etwa Beatmungsgeräte (unbeschadet der Beantwortung der derzeit aufkeimenden Frage des medizinischen Nutzens) und Großgeräte zur Bekämpfung der Pandemie zu beschaffen.

Hierzu hat die Deutsche Röntgengesellschaft, Gesellschaft für medizinische Radiologie e.V. sich bereits zur Frage der unterstützende Diagnostik durch die Computertomographie (CT) dahingehend geäußert, dass dies eine wertvolle Hilfe bei der Diagnose sowie der Einschätzung des Schwergrads und Verlaufs von COVID-19 und von Pneumonie-assoziierten Komplikationen sei. Nur bei Verdacht auf eine COVID-19 Infektion aufgrund einer ausgeprägten respiratorischen Symptomatik (z. B. Atemnot), die eine Hospitalisierung erfordert sowie einer negativen RT-PCR kann die Thorax-CT die Diagnose frühzeitig stützen.

Die wichtigste Aufgabe der CT im Rahmen der COVID-19-Pandemie ist die Diagnose von Pneumonie-assoziierten Komplikationen sowie die Bewertung des initialen Krankheitsausmaßes und die Verlaufsbeurteilung. Sie unterstützt damit die klinische Einschätzung von besonders schweren Erkrankungsfällen. Aufgrund dieser Einsatzspezifikation kann ebenfalls Dringlichkeit in der Beschaffung angenommen werden.

Situationsbedingte Änderungen in Beschaffung von Medizinprodukten (Verbrauchsmaterial)

Aufgrund der pandemischen Ausbreitung des Virus mit der Bezeichnung SARS-CoV-2 liegen die Voraussetzungen des § 14 Abs. 4 Nr. 3 Vergabeverordnung (VgV) vor, so dass ein Verhandlungsverfahren ohne Teilnahmewettbewerb zulässig ist. Mit dieser Erleichterung fangen die Fragen erst an.

Allein die Aussage, dass eine weniger geregelte Vergabe zulässig ist, führt zu Begehrlichkeiten, auf ein geregeltes Verfahren zu verzichten. Allerdings sind die Verfahrensvorgaben aus dem Vergabe- und Haushaltsrecht einzuhalten. Das Verfahren der Verhandlungsvergabe ohne Teilnahmewettbewerb richtet sich nach § 17 Abs. 5 VgV; die ausgewählten Unternehmen werden unmittelbar angesprochen; für den Bereich unterhalb der Schwellenwertes von 214.000,- € sieht § 12 Abs. 2 der Unterschwellenvergabeordnung (UVgO) vor, dass mindestens 3 Bieter aufgefordert werden. Zulässig ist es jeweils, sich vorzubehalten, den Zuschlag auf das Erstangebot zu erteilen.

Fazit

Die Sars-CoV-2-Pandemie ist ein Beispiel für die Flexibilität des Vergaberechtes. Bei der Bewältigung der durch diese Virus-Infektion auftretenden Krankheitsbilder ist stets von Dringlichkeit im Sinne des Vergaberechts auszugehen. Eine andere Frage ist die, ob es genügend Produkte am Markt wie etwa Schutzmasken, gibt. Durch eine strukturierte Abarbeitung im Beschaffungsprozess wird eine zeitgerechte Bereitstellung der notwendigen Materialien im Krankenhaus dringend empfohlen, soweit die Produkte am Markt erhältlich sind.

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

IT Sicherheit im Krankenhaus

Journal für Strategie und Praxis

Die Zeichen stehen auf *Wandel*

Die Information Security in Healthcare Conference findet am Donnerstag, 4. Juni 2020, im neuen Campus der Hochschule Luzern in Rotkreuz statt. Das Thema "Prävention gegen die Erkrankung von Gesundheits Daten" ist hochaktuell und brisant wie nie. Das Krankenhaus-IT Journal sprach im Vorfeld mit *Erwin N. Schnee*, Organisator der Information Security in Healthcare Conference.

Erwin N. Schnee, Organisator der Information Security in Healthcare Conference

Welche Idee steckt hinter der Information Security in Healthcare Conference?

Die Information Security in Healthcare Conference wurde vor fünf Jahren anlässlich eines Gedankenaustausches zwischen Prof. Peter E. Fischer von der Hochschule Luzern und mir geboren. Wir hatten festgestellt, dass es im Gesundheitswesen zwar eine Vielzahl von Veranstaltungen und Konferenzen gibt, doch der Bereich Informationssicherheit wurde meist, wenn überhaupt, nur am Rande thematisiert. Es gab zu diesem Zeitpunkt große Veranstaltungen, die sich diesem Thema sogar kategorisch verweigerten.

Aufgrund einer detaillierten Marktanalyse haben wir uns entschieden, ein Konzept für diese Konferenz auszuarbeiten. Auch nach persönlichen Gesprächen mit Anbietern von Lösungen im Bereich Informationssicherheit im Gesundheitswesen wurde uns bestätigt, dass hier in Zukunft ein großer Bedarf vorhanden ist.

Wann fand die Konferenz erstmalig statt und wie war die Resonanz?

Im Januar 2015 erhielten wir von der Hochschule Luzern (HSLU) das Go für die Information Security in Healthcare Conference. Die erste Konferenz fand im Juni 2015 statt. Es versteht sich von selbst, dass wir uns einen sehr ambitionierten Zeitplan gestellt haben. Alles musste von Grund auf neu entwickelt und gestaltet werden. Das Logo, die Webseite, die Sponsoren-, sowie die Teilnehmergewinnung, etc.

Die erste Konferenz konnte 2015 mit rund 70 Teilnehmern, 4 Partnern und 8 Referenten durchgeführt werden. In 2020, also fünf Jahre später, werden bereits 300 Teilnehmer, 20 Partner und 25 Referenten erwartet.

Nach welchen Kriterien wählten Sie den Veranstaltungsort?

Für Rotkreuz als Veranstaltungsort gibt es verschiedene Gründe. Die meisten Veranstaltungen in der Schweizer Healthcare Szene finden in Zürich oder Bern statt. Es war bekannt, dass die HSLU Fachgebiet Informatik ab 2017 den Betrieb in einem Provisorium in Rotkreuz aufnehmen würde. 2019 sollte dann der jetzige Standort bezogen werden können. Einen Ausbildungsschwerpunkt der HSLU bildet das Thema Information Security und die HSLU war der erste Träger der Konferenz. Rotkreuz ist ein Eisenbahnknotenpunkt in der Schweiz. Somit ist die Veranstaltung aus der gesamten deutschsprachigen Schweiz innert 1 1/2 Stunden mit dem öffentlichen Verkehr erreichbar. Zudem sind der alte und der neue Austragungsort nur rund 150 m vom Bahnhof entfernt. Von allem Anfang an wurden wir von der Gemeinde unbürokratisch unterstützt. Kommt dazu, dass es in der Gemeinde Rotkreuz im Bereich HealthTech und Pharma gegen 3500 Arbeitsplätze gibt und dieser Zweig seit Jahren schnell wächst.

Mit dem Umzug der Konferenz in den Campus der HSLU profitieren wir nun von einer modernen Infrastruktur.

Welche Veranstaltungspartner unterstützen die Konferenz? Welche Schwerpunkte gibt es?

Nach der Information Security in Healthcare Conference 2018 ist die HSLU als Träger ausgestiegen, da sie Konferenzen nicht als eine ihrer Kernkompetenzen betrachtet. Dank den neuen Trägern, des Health Tech Cluster Switzerland (HTCS) und der Information Security Society Switzerland (ISSS), ist es uns gelungen, zwei kompetente Veranstaltungspartner zu finden, die uns weiterbringen und sich gegenseitig ergänzen.

Jedes Jahr stellen wir die Konferenz unter ein anderes Thema. Dabei versuchen wir bewusst Bereiche zu wählen, die sowohl in der IT als auch Medizin gebräuchlich sind. Dieses Jahr lautet der Titel «Prävention gegen die Erkrankung von Gesundheitsdaten». Daten/Datencontainer werden in Zukunft an Bedeutung gewinnen. Denken wir nur an die personalisierte Medizin, Biobanks etc. Es ist auch anzunehmen, dass konventionell gespeicherte Informationen nun laufend digitalisiert werden. Ein Beispiel sind hier Pathologieresultate. Die grössten Datenpools nützen nichts, wenn es sich um erkrankte oder gestohlene Daten handelt. Also gewinnt die Informationssicherheit in den nächsten Jahren an Bedeutung. Ich spreche hier klar von

Informationssicherheit und nicht Cybersicherheit, weil die Informationssicherheit viel umfassender ist.

Was können die Teilnehmer auf der Konferenz erwarten? Welche Highlights stehen auf der Agenda?

Auf der einen Seite ist jedes der vier Keynote-Referate für sich sehr speziell. Auf der anderen Seite werden unterschiedliche Themengebiete angesprochen.

Adrian Schmid von eHealth Swiss berichtet über die aktuelle Situation bei der Einführung des elektronischen Patienten Dossiers in der Schweiz und streift den Bereich Verordnungen in der Medizinaltechnik.

Prof. Kurt Zatloukal von der Medizinischen Universität Graz wird das Publikum über seine Erfahrungen mit der Fragmentierung von Daten und Bildern informieren. Weiter wird er aufzeigen, wie sich solche Informationen in Zukunft zum Patientennutzen einsetzen lassen.

Dr. Nicolas Krämer von der Rheinland Klinikum Neuss GmbH berichtet über seine Erfahrungen als kaufmännischer Leiter. Was passiert, wenn von einem Tag auf den anderen von digitalen Prozessen auf Bleistift und Block umgestellt werden muss? Nebst den rein internen Problemen geht es um die Kommunikation an die breite Öffentlichkeit, den Patienten, den Medien, der Politik usw.

Stefan Juon wird als CISO des Kantonsspital Graubünden seine Erfahrungen im Umgang mit Cybersecurity weitergeben.

Aber nicht nur die Keynote-Referate sind spannend, sondern auch die einzelnen Stream-Referate werden Neuigkeiten bringen. Das geht von der Emotet Attacke auf Kliniken über neue Leitsysteme für Spitäler bis zu Awareness Kampagnen und die Thematik IoMT (Internet of Medical Things). Viele der Stream-Referenten dürfen von effektiven Geschehnissen berichten. Häufig werden negative Ereignisse im Gesundheitswesen unter Verschluss gehalten.

Welche Themen wurden auf vergangenen Konferenzen behandelt und wie war die Resonanz?

Bei den ersten zwei Konferenzen ging es stark um Themenstellungen im Bereich Datenschutz und das Patientendossier. Ab 2017 haben wir bewusst Themen rund um die Informationssicherheit gewählt «Cyber Crime gefährdet Leben». 2018 hatten wir ein Highlight: mit einen Livehack und der Veränderungen der Vitaldaten im HL7 Protokoll. Diese Problematik war so brisant, dass noch am selben Tag in der Hauptausgabe der Nachrichten des Schweizer Fernsehens SRF ein Bericht über die Konferenz ausgestrahlt wurde. 2019 war der Titel der Konferenz "protect – detect – respond". Detaillierter Information finden Sie Ausgabe von Krankenhaus IT 3/2019.

Seitens der Organisation wird die gesamte Konferenz laufend detailliert analysiert. Generell wird der Anlass als gut bis sehr gut bewertet. Bei den Referaten haben wir teils große Schwankungen. Was wir aber sagen können, je näher der Redner an der Praxis ist, umso besser fällt die Bewertung seines Vortrages aus. Referenten, die einen zu starken Fokus auf das eigene Unternehmen und deren Produkte legen, werden weniger positiv beurteilt. Schlecht schneiden auch globale Referate mit internationalen Folien und wenig Bezug zu den lokalen Gegebenheiten ab. Dieses Bewertungsschema führt dazu, dass gewisse Unternehmen die Konferenz seit Jahren mit starken Vorträgen bereichern und so wertvolle Kontakte knüpfen können. Schwächere Referate führen dazu, dass der Referent sein Netzwerk kaum erweitern kann.

Wie sehen Sie die Zukunft Ihrer Veranstaltung? Was erhoffen Sie sich im Nachgang?

Eine weitere Eigenheit der Information Security in Healthcare Conference ist, dass wir als eine der wenigen Veranstaltungen weitestgehend auf Messestände verzichten. Stattdessen schaffen wir sogenannte Themeninseln mit dem Ziel, dass sich hier Referenten und Besucher zum Erfahrungsaustausch treffen. Ganz generell wird der Austausch zwischen Teilnehmern untereinander sowie deren Dialog mit den Rednern großgeschrieben. Beobachtungen zeigen, dass dies gelingt, weil die Besucher nicht das Gefühl haben, jeden Moment durch einen Verkäufer angesprungen zu werden.

Wir machen uns laufend Gedanken, was wir verbessern können. Eines können wir sagen: Diese Konferenz ist wichtig, um der Informationssicherheit im Gesundheitswesen ein Gesicht zu geben. In Gesprächen mit Leistungserbringern höre ich oft die Klage, dass das Spitalmanagement und operative Stellen der Information Security wenig Bedeutung beimessen. Entsprechend sieht es bei der Budgetverteilung aus. Hier leistet die Konferenz einen Beitrag, um langsam, aber stetig einen Wandel anzustoßen.

In Zukunft wird es die Konferenz in dieser Form als Leuchtturm-Veranstaltung weiterhin geben. Wir stellen aber fest, dass es nicht reicht, einmal pro Jahr einen Anlass zu organisieren. Deshalb arbeiten wir zurzeit an Möglichkeiten, kleinere themenspezifische dezentrale Informationsveranstaltung zu lancieren. Wir bilden gerne die Brücke zwischen Lösungsanbietern und Anwendern. Natürlich sind wir darauf angewiesen Partner zu haben, um die Anlässe finanzieren zu können.

Die diesjährige Coronavirussituation zeigt uns zudem auf, wie verletzlich Konferenzen durch äußere Einflüsse sein können. Das ist ein Grund, weshalb wir uns intensiv mit der Möglichkeit von Hybridveranstaltungen, also einer Liveveranstaltung kombiniert mit Streaming, befassen. Reine Streaming Lösungen schauen wir uns ebenfalls näher an. Wobei wir hier die Möglichkeit prüfen müssen, wie sich der persönliche Dialog zwischen Teilnehmern untereinander als auch mit den Referenten realisieren lässt.

Safety und Security müssen zusammenwachsen

IT-Sicherheit in Krankenhäusern

Wenn Cyberangriffe auf Krankenhäuser in die Schlagzeilen geraten, ist die öffentliche Bestürzung groß. Diese Vorfälle sind besonders erschreckend, weil die Auswirkungen konkret und leicht fassbar sind. Und mitunter sogar lebensbedrohlich. Nach solchen Angriffen fordern die Verantwortlichen meist Geld, um die IT in Kliniken besser zu schützen. Aber wären Finanzspritzen das Allheilmittel? Rico Barth hat mit seinem Unternehmen, dem IT-Dienstleister cape IT aus Chemnitz, schon in mehreren Krankenhäusern nicht nur die IT aufgebaut, sondern gleichzeitig auch die Cybersecurity auf den neuesten Stand gebracht. Im Interview spricht er über Risiken für die Krankenhaus-IT, Gesetzeslücken und Lösungsansätze.

Rico Barth Geschäftsführer cape IT

Warum sind gerade Krankenhäuser leichte Opfer für IT-Angriffe? Hinkt bei diesen Institutionen der digitale Schutz noch besonders hinterher?

Krankenhäuser sind nun mal grundsätzlich offene Gebäude, die jeder ohne Weiteres betreten kann. In Gerichten und Gefängnissen gibt es Personenkontrollen und andere Sicherheitsmaßnahmen. Aber der Zweck einer Klinik erfordert eben radikale Offenheit, die trotzdem abgesichert werden muss. Management, Chefärzte und das gesamte Personal müssen dafür sensibilisiert werden. In der Industrie zum Beispiel lag lange Zeit der Fokus auf der Optimierung der Produktionsprozesse und erst jetzt, im Zuge von Industrie 4.0, nehmen die Verantwortlichen die IT-Sicherheit in der gesamten Prozesskette ins Visier. In Kliniken liegt dafür der Schwerpunkt auf Medizinequipment. Die IT ist einfach nur Mittel zum Zweck, sie muss funktionieren und macht eigentlich nur auf sich aufmerksam, wenn es mal Probleme gibt. Der Blick auf die IT sollte sich auch hier wandeln: hin zu einer proaktiven, vorausschauenden Umgangsweise. Da stehen wir noch ganz am Anfang.

Im Juli 2019 mussten sich DRK-Krankenhäuser in Rheinland-Pfalz und im Saarland gegen einen Hackerangriff zur Wehr setzen. Das komplette Netzwerk des 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. War das der richtige Schritt?

Ja, das war sogar ein notwendiger Schritt. Größere Kliniken, die in einem Verbund organisiert sind, beschäftigen sich schon lange mit dem Thema IT-Sicherheit und sind daher hier besser aufgestellt: Sie haben mehr IT-Budget, geschultes Personal und das Management ist sensibilisiert, nicht zuletzt durch die vermehrten Hackerangriffe auf Krankenhäuser in den letzten Jahren. Kleinere Häuser investieren spürbar weniger. Oft, weil ihnen schlicht das Geld fehlt und sie eh schon an allen Ecken und Enden sparen. Bisher waren bei Angriffen immer sensible Daten beziehungsweise die Verwaltung betroffen. Gar nicht auszudenken, was passiert, wenn Hacker ganze Systeme übernehmen. Da sind sehr schnell Leben in Gefahr.

Größere Krankenhäuser müssen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) über ihre Maßnahmen gegen Cyberkriminalität und Angriffe gegen ihre Systeme Bericht erstatten, erhalten aber auch mehr Geld für die IT-Sicherheit. Wie gestaltet sich die Situation für kleinere Krankenhäuser?

Kleinere Krankenhäuser in ländlichen Gegenden sind häufig die einzige Notfallversorgung für eine ganze Region. Sie stellen ebenso eine ‚kritische Infrastruktur' dar wie größere und besser ausgestattete Kliniken. Allerdings stuft der Gesetzgeber sie momentan nicht so ein. Sie müssen weniger strenge IT-Auflagen erfüllen, aber ihnen fehlen eben auch Ressourcen. Im Kampf gegen Cyberkriminalität sind sie deshalb absolut benachteiligt. Vorschriften zur IT-Sicherheit sollten für alle Häuser gelten. In der TÜV-Cybersecurity-Studie, die der TÜV-Verband Anfang November vorgestellt hat, wird auch genau das und sogar mehr eingefordert: eine Ausweitung des IT-Sicherheitsgesetzes auf alle Bereiche der Wirtschaft, über die kritische Infrastruktur hinaus. Knapp zwei Drittel der befragten Unternehmer waren sich einig, dass gesetzliche Bestimmungen entscheidend für die IT-Sicherheit in Deutschland sind. Und natürlich sollten die kleineren Krankenhäuser dann auch entsprechend vom Staat mit Geld ausgestattet werden. Warum sollte man hier einen Unterschied machen? Am Menschen wird in jeder Klinik gearbeitet, egal ob klein oder groß, in der Stadt oder auf dem Land.

Müssen Sie bei Krankenhäusern höhere Sicherheitsstandards einhalten als bei anderen Kunden? Stellt Sie das als IT-Dienstleister vor besondere Herausforderungen?

Security Management Systeme direkt einzubinden, ist heute absolut gefordert und nicht mehr nur ‚nice to have'. Mit unserer Software KIX geht es uns darum, sämtliche Prozesse unserer Kunden zu unterstützen und bei Bedarf zu automatisieren, sei es IT, Haustechnik oder auch Medizingerätetechnik. Ziel ist es dabei, alle Bereiche mit individuellen Lösungen abzudecken – eine homogene IT-Monokultur wäre sogar eher eine Gefahr. Jede Klinik verfügt schon jetzt über eine gewachsene IT-Infrastruktur. Es bietet sich an, diese spezialisierten Lösungen über offene Schnittstellen miteinander kommunizieren zu lassen und nahtlos in ein IT-Sicherheitsmanagement zu integrieren, natürlich nach dem BSI-Standard.

Was können Krankenhäuser präventiv tun, um sich vor Cyberangriffen zu schützen? Sofort und mittelfristig?

Die Anforderungen des IT-Grundschutz vom BSI decken schon recht viel ab. Sie müssen nur durchgesetzt werden, was ja auch sukzessiv erfolgen kann. Der spezielle Sicherheitskatalog B3S der Deutschen Krankenhausgesellschaft gibt Kliniken aller Größen einen Fahrplan an die Hand, um diesen Umbruch zu bewältigen. Wichtig ist zum Beispiel die sogenannte Härtung des Serversystems. Das System muss so schlank wie möglich gehalten werden, um Hackern keine Einstiegsmöglichkeiten zu bieten. Der Einsatz von Open Source Software ist dabei unbedingt zu empfehlen, denn so kann jeder Nutzer den Quellcode einsehen und auf Risiken und Schwachstellen überprüfen. Jedes Krankenhaus behält damit seine digitale Souveränität. Selbstverständlich gehört auch eine Einbeziehung des Personals dazu: Nicht nur im Alltag müssen sie souverän mit der IT umgehen können, sie müssen genau wie auf Brände und Naturkatastrophen auch auf Cyberangriffe vorbereitet werden.

Medizinische Geräte werden immer häufiger in Netzwerke integriert, so dass etwa Ärzte aus anderen Krankenhäusern Geräte übers Internet steuern können. Sobald sie einmal zertifiziert sind, dürfen sie aber nicht verändert werden, das heißt, auch keine Sicherheitsupdates ausführen. Wie können Krankenhäuser ihre Anti-Viren-Software trotzdem aktuell halten?

Sicherheitsupdates sind wichtige Vorsorgemaßnahmen in der IT. Da wir digital immer komplexer zusammenwachsen, gilt das auch für alle Bereiche, die durch IT miteinander verbunden sind. Mit diesem Dilemma hat auch zum Beispiel auch Tesla zu kämpfen, sie dürfen eigentlich keine Sicherheitsupdates an ihren Autos durchführen. Die zentrale Bundesbehörde muss die bisherigen Regelungen dringend auf den Prüfstand stellen und an aktuelle technische Entwicklungen anpassen.

Waren Sie vor besondere Herausforderungen gestellt, um bei Ihren Kunden Medizingeräte in die IT-Administration einzubinden? Können Sie da inzwischen auf eine ‚Schablone' zurückgreifen oder ist jeder Fall individuell?

Mittlerweile sind medizinische Geräte und IT-Equipment stärker verwoben als noch vor einigen Jahren. Früher war bei einem Medizingerät nur die Safety zu bedenken, also der Schutz von Mensch und Umwelt vor physischem Schaden. Jetzt müssen wir auch die Security, insbesondere die IT-Security, gewährleisten. Safety und Security wachsen zusammen, genauso wie IT, Medizingerätetechnik und Gebäudeautomation. Das birgt Risiken, aber vereinfacht auch die Konfiguration und die Überwachung. Da Medizingeräte nach identischen Standards kategorisiert sind, haben wir mittlerweile eine gute Blaupause entwickelt, um die Medizingeräteverwaltung einzurichten. Und das sowohl in den Abläufen wie zum Beispiel der Mitarbeitereinweisung als auch der Dokumentation, also den Geräte-Logbüchern.

Obwohl Einigkeit darüber herrscht, dass IT-Sicherheit immens wichtig ist, scheint es für die meisten Menschen, auch dem Krankenhauspersonal, eher ein lästiges Thema zu sein. Erleben Sie das auch so?

Zum Teil zumindest. In den letzten Jahren hat da sicherlich ein Umdenken begonnen, aber manchmal wünsche ich mir, dass es schneller geht. Der Chefarzt ist und bleibt natürlich in erster Linie Mediziner. Wenn der sich ein neues Röntgengerät anschafft, denkt er nicht automatisch daran, was das für Arbeitsprozesse in der IT-Abteilung und beim technischen Personal in Gang setzt. So ein Röntgengerät hat ja auch einen Netzwerkanschluss und muss in ein System eingepflegt werden, die Mitarbeiter müssen eingewiesen, das Gerät muss gewartet und das Ganze muss regelmäßig wiederholt werden. Und natürlich alles mit lückenloser Dokumentation. Hier können wir mit KIX, unserem Service Management System, helfen, strukturierte Arbeitsabläufe und eine sichere Betriebsführung zu ermöglichen. So wird die Dokumentation quasi automatisch erledigt. Spätestens wenn der Auditor seinen jährlichen Besuch im Krankenhaus abstattet und eine 1A-Dokumentationslage vorfindet, werden alle Krankenhausmitarbeiter dankbar für diesen Service sein.

Über cape IT:

Die c.a.p.e. IT GmbH ist Hersteller und Dienstleister der eigenen Open Source Service Software KIX, die vielseitigen Einsatz vor allem im technischen Service & IT Service Management findet. Dabei liegt der Fokus auf der individuellen Unterstützung bei Analyse, Implementierung und Anpassung an kundenspezifische Anforderungen. Das Unternehmen mit Stammsitz in Chemnitz wurde 2006 als Spin Off eines international tätigen IT-Systemhauses gegründet. c.a.p.e. IT beschäftigt aktuell knapp 50 erfahrene, ITIL-zertifizierte Mitarbeiter an zwei Standorten und engagiert sich in den Branchenverbänden der Open Source Business Alliance, BITKOM und itSMF.

Das Internet der Dinge bietet große Chancen – birgt aber auch Gefahren

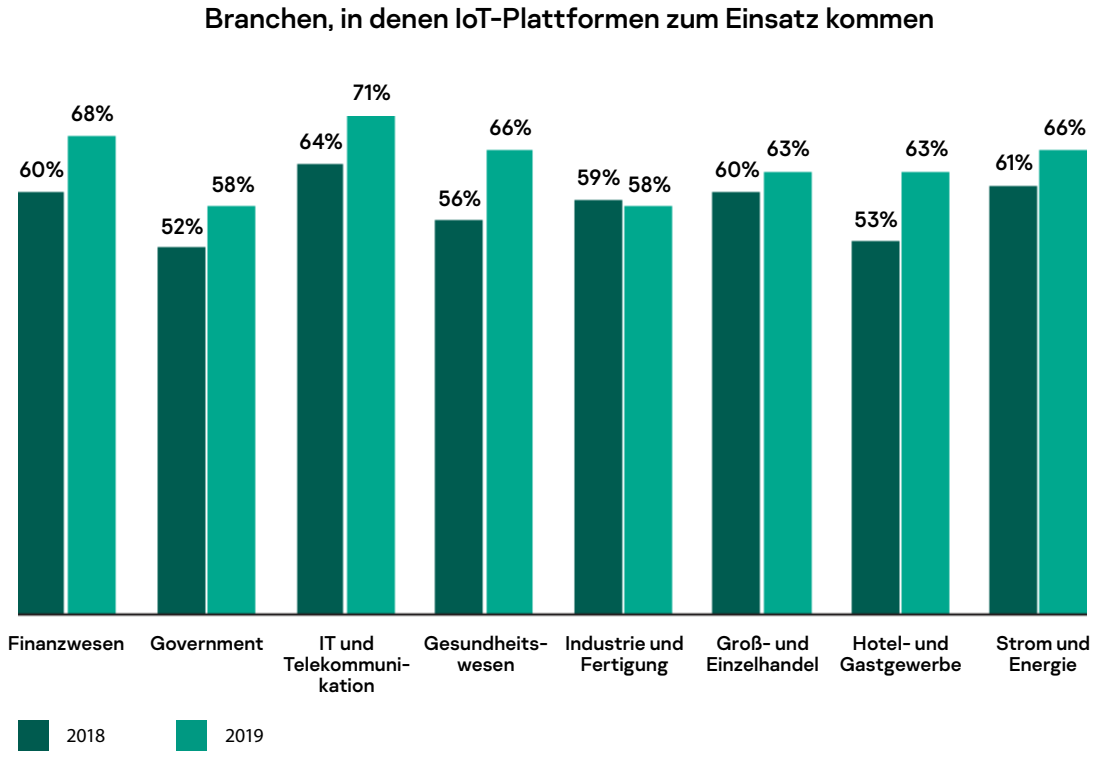
IoT im Gesundheitswesen

Ob MRT-Scanner, Krankenhaus-Logistik oder Wearables, das Internet der Dinge (IoT) hält auch in der Gesundheitsbranche zunehmend Einzug. Dies bestätigt eine aktuelle Studie des IT-Sicherheitsspezialisten Kaspersky [1] hinsichtlich des Einsatzes und der kurz- und mittelfristigen Herausforderungen in puncto IT-Sicherheit im Bereich IoT.

Innerhalb der Studie „With superpower comes super responsibility: Benefits and challenges of IoT in business" wurde unter anderem der Einsatz von IoT in der Gesundheitsbranche untersucht. Das Ergebnis: 66 Prozent der befragten Einrichtungen und Unternehmen aus dem Healthcare-Bereich setzen IoT-Plattformen für ihre Geschäftsanwendungen ein. Dies bedeutet einen Anstieg um zehn Prozentpunkte im Jahr 2019 gegenüber 2018. Im Vergleich zu anderen Branchen – etwa dem IT- und Telekommunikationssektor, der mit 71 Prozent den höchsten IoT-Nutzungswert aufweist – liegt der Gesundheitsbereich mit lediglich fünf Prozentpunkten Differenz dahinter.

Mit den durch den Einsatz von IoT gewonnenen Vorteilen, wie die Erschließung neuer Geschäftsfelder oder einer modernen Patientenbetreuung, gehen allerdings auch größere Anforderungen im Hinblick auf die Themen Cybersicherheit und Datenschutz einher. Allein in der ersten Jahreshälfte 2019 identifizierten die Experten von Kaspersky weltweit 105 Millionen Angriffe auf IoT-Geräte [2]. Zudem waren im Jahr 2019 ein Fünftel (19 Prozent) aller Computer und Geräte (nicht nur IoT) in medizinischen Einrichtungen einem Infektionsversuch ausgesetzt. Die neue Studie unterstreicht zudem, dass zunehmend IoT-Systeme von Cyberbedrohungen betroffen sind. So gaben branchenübergreifend 28 Prozent der Befragten an, im Jahr 2019 IT-Sicherheitsprobleme im Zusammenhang mit der Nutzung von IoT-Plattformen gehabt zu haben.

Hinzu kommt, dass vernetzte Geräte und Sensoren Daten – unter anderem auch kritische Geschäftszahlen oder sensible Patientendaten – im Terabyte-Bereich übertragen. Der Bereich Drittanbieter und Zulieferer spielt hierbei eine nicht unwesentliche Rolle. Im Hinblick auf das eigene Partnersystem gaben nämlich – ebenfalls branchenübergreifend – 36 Pro-



zent der Umfrageteilnehmer an, externen Partnern Zugriff auf ihre betriebseigene IoT-Plattform zu gewähren. Dies ist – gegenüber den entsprechenden Prozentwerten auf Produktions- und ERP-Software mit 23 und 30 Prozent – ein merklich höherer Wert. Insbesondere im Gesundheitswesen gilt es, auf den Schutz persönlicher Patientendaten zu achten, die unmittelbar mit IoT-Geräten in Verbindung stehen. So ergab eine Recherche des Bayerischen Rundfunks und ProPublica [3] aus dem vergangenen Jahr, dass hochsensible medizinische Informationen, unter anderem von Patienten aus Deutschland und den USA, auf ungesicherten Servern gelandet sind. Darunter befanden sich Millionen medizinischer Bilder und Gesundheitsdaten wie Röntgen-, MRT- und CT-Aufnahmen von Menschen weltweit. Da die Server komplett ungeschützt waren, hätte theoretisch jeder Zugriff auf diese vertraulichen Datensätze gehabt.

Ransomware-Angriffe vorbeugen

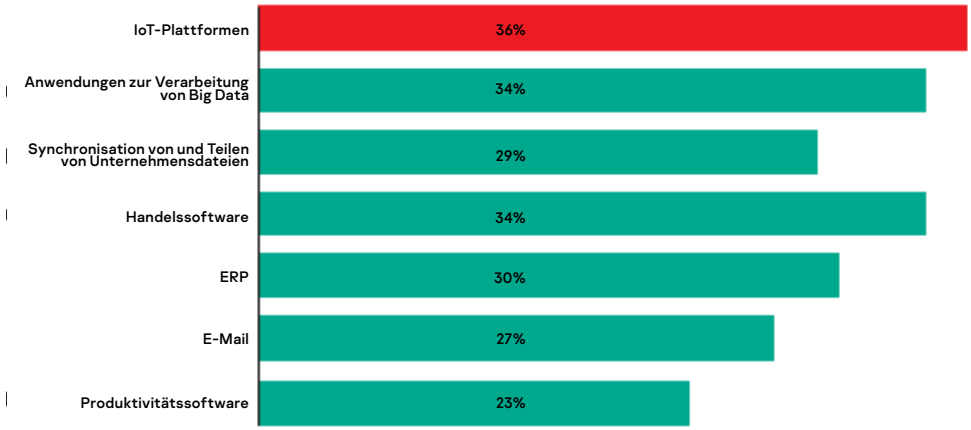
Der Erpressungs-Trojaner WannaCry legte bereits im Jahr 2017 die IT zahlreicher Krankenhäuser in England lahm. Die hinter dieser Aktion stehenden Cyberkriminellen sperrten damals eine Vielzahl von Computern, die nur gegen die Zahlung eines Lösegelds wieder freigegeben wurden. Um zu vermeiden, dass sich ein solches Ransomware-Szenario für das Internet der Dinge im Gesundheitswesen wiederholt, ist es wichtig, dass Anbieter von IoT-Technologie adäquaten Cyberschutz in ihren Produkten implementieren.

Darüber hinaus liegt es in der Verantwortung der Anwender, ein sicheres, stets auf dem neuesten technologischen Stand

Christian Milde, General Manager DACH bei Kaspersky

gehaltenes IoT-System aufzubauen. Um das Risiko eines Cyber-Sicherheitsvorfalls zu minimieren, sollten Organisationen daher sicherstellen, dass ihr gesamtes Netzwerk und ihre Geräte sowie die Software ordnungsgemäß vor digitalen Gefahren von außen geschützt sind.

Geschäftsanwendungen, auf die von Dritten zugegriffen wird



Maßnahmen für mehr IoT-Sicherheit

Für eine sichere und erfolgreiche Nutzung von IoT-Technologien sollten Einrichtungen und Unternehmen aus dem Healthcare-Bereich folgende Punkte beachten:

1.) Vor dem Einsatz von vernetzten Geräten muss deren Sicherheit evaluiert werden. Haben die Geräte Sicherheits-Zertifikate? Ist der Hersteller bekannt für sein Augenmerk auf Informationssicherheit?

2.) Das für die IT-Sicherheit verantwortliche Team sollte über aktuelle Threat-Intelligence-Kenntnisse verfügen. Sicherheits-Audits müssen regelmäßig durchgeführt werden.

3.) Eine geeignete und rasche Vorfallreaktion setzt voraus, dass Verfahren eingeführt werden, mit deren Hilfe stets aktuelle Informationen über wesentliche Sicherheitslücken innerhalb der Software, in Anwendungen sowie zu verfügbaren Updates bereitgestellt werden.

4.) Der Einsatz leistungsstarker Cybersicherheitslösungen, die den Netzverkehr analysieren und mögliche Angriffe auf IoT-Geräte erkennen und verhindern können, ist essentiell. Die auf diese Weise gewonnenen Erkenntnisse können dann in das komplette Netzwerksicherheitssystem des Unternehmens einfließen.

5.) Zum Einsatz sollten nur IoT-Geräte kommen, die speziell auf Sicherheit ausgelegt sind. Die Lösung Kaspersky IoT Secure Gateway [4] – mit KasperskyOS als Herzstück – gewährleistet ein sicheres Gateway und schützt alle verbundenen Geräte sowie das komplette IoT-System.

[1] https://kas.pr/6gmw
[2] https://securelist.com/iot-a-malware-story/94451/ und https://securelist.com/healthcare-predictions-2020/95385/
[3] https://www.tagesschau.de/investigativ/br-recherche/

Weitere Informationen zum Lösungsportfolio von Kaspersky im Gesundheitswesen:
www.kaspersky.de/enterprise-security/healthcare

Die Sicherheitsexperten von Kaspersky prognostizieren neben IoT-Risiken die folgenden Cyber-Herausforderungen, auf die sich die Gesundheitsbranche in näherer Zukunft einstellen sollte:

- ***Patientendaten werden im Darknet verstärkt nachgefragt.*** Sensible Gesundheitsdaten werden im Cyberuntergrund zum Teil bereits teurer als Kreditkartendaten gehandelt. Dies eröffnet auch neue potenzielle Betrugsmethoden, denn durch den Besitz solch sensibler medizinischer Informationen wird es einfacher, Betroffene und Angehörige zu betrügen.
- ***Modifizierung von Patientendaten.*** Ein potentieller Zugriff auf Patientendaten ermöglicht nicht nur den Diebstahl derselben, sondern erhöht auch die Gefahr von Modifizierungen der entsprechenden Informationen. Mögliche Folgen sind zielgerichtete Angriffe auf Einzelpersonen, indem die Diagnose verfälscht wird – mit möglicherweise tödlichen Folgen.
- ***Angriffe gegen medizinische Einrichtungen.*** Im kommenden Jahr werden mehr Cyberangriffe auf Geräte medizinischer Einrichtungen in Ländern zu beobachten sein, die am Anfang des Digitalisierungsprozesses medizinischer Services stehen – beispielsweise zielgerichtete Ransomware-Attacken gegen Krankenhäuser in Entwicklungsländern.
- Auch wird es voraussichtlich vermehrt zu ***zielgerichteten Attacken auf medizinische Forschungsinstitute und Pharmaunternehmen***, die innovative Forschung betreiben, kommen.
- ***Cyberangriffe gegen medizinische Implantate.*** Was nach Zukunftsmusik klingt, steht bereits in den Startlöchern. Medizinische Implantate weisen Schwachstellen auf, die schon bald von Cyberangreifern ausgenutzt werden könnten. Diese neue Gefahr wird durch den Aufbau zentralisierter Netzwerke von Wearables und medizinischer Implantate umso wahrscheinlicher.

10 goldene Regeln für ein sicheres Home Office

IT-Sicherheit für das Arbeiten zuhause

Ein großer Teil der deutschen Angestellten arbeitet derzeit von zuhause aus – vom Sachbearbeiter bis zum Geschäftsführer. Das bringt in vielen Fällen neue IT-Sicherheitsrisiken mit sich. Auch Hacker nutzen die aktuelle Unsicherheit verstärkt aus. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits Alarm geschlagen.

Die Anbindung des Heimarbeitsplatzes erfolgte in den meisten Unternehmen von jetzt auf gleich, also ohne die erforderlichen Vorbereitungen. Videokonferenzen, Cloud-Anwendungen und mobile Endgeräte bieten zwar eine enorme Erleichterung für die dezentrale Zusammenarbeit. Doch eröffnen sich für Cyberkriminelle durch diese Infrastrukturen auch neue Angriffspunkte. Hinzu kommen zigtausende veralteter Computer, ungesicherter Router und schlecht geschützter WLAN-Verbindungen, die mit einem Mal Zugang zu den sensiblen Daten von Unternehmen bieten. Wie aber können Unternehmen unter diesen Bedingungen die Heimarbeitsplätze ihrer Mitarbeiter trotzdem erfolgreich vor Hackerangriffen schützen? Dies zeigen die folgenden 10 goldenen Regeln:

1. Alle Mitarbeiter, die an das Unternehmensnetzwerk angebunden sind, sollten verbindliche und eindeutige Regelungen für den Schutz der IT und der Daten im Unternehmen erhalten – und zwar schriftlich.

2. Endgeräte vor Angriffen aus dem Internet schützen. Der aktuelle Informationsbedarf in der Corona-Krise wird verstärkt von Hackern ausgenutzt. Über gefälschte Webseiten, Emails oder Grafiken, die aus scheinbar vertrauensvollen Quellen stammen, wird Malware auf Rechner geschleust. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt Bürger und Unternehmen vor der Zunahme solcher Angriffe. Der beste Schutz vor Angriffen aus dem Internet ist ein virtueller Browser, den das BSI entwickeln ließ. Kommt dieser zum Einsatz haben Cyber-Kriminelle keine Chance. Mehr dazu im Infokasten „Sicheres Browsen".

3. Daten auf den Endgeräten schützen. Vor allem Organisationen mit hohen Sicherheitsanforderungen sollten die Endgeräte ihrer Mitarbeiter mit einer Festplattenverschlüsselung ausstatten. Nur berechtigte Nutzer können dann per Multi-Faktor-Authentifizierung ihre Daten und das Betriebssystem nutzen. Geht das Gerät verloren oder wird es gestohlen, ist es für Dritte nicht möglich, auf die Daten zuzugreifen.

4. Grundlegende Sicherheitsmaßnahmen. Der Arbeitsplatz in den eigenen vier Wänden sollte physisch gesichert werden, indem Türen verschlossen und Bildschirme gesperrt werden. Empfehlenswert ist zudem, die Webcam am Rechner oder Laptop abzudecken, wenn diese nicht benötigt wird, sowie bei Nichtgebrauch das Mikrofon auszuschalten, um mögliche Spionageattacken ins Leere laufen zu lassen.

5. Heimische WLAN-Verbindung absichern. Das Standard-Administrator-Passwort sollte durch ein neues, starkes Passwort ersetzt und die WPA2-Verschlüsselung aktiviert wird.

6. Betriebssysteme, Webanwendungen und Apps aktualisieren. Alle IT-Technologien eines Unternehmens müssen auf dem aktuellsten Stand sein – das ist ein wesentlicher Schutz vor Hackern. Alle Mitarbeiter sollten daher regelmäßig Updates ausführen und mit der neuesten Systemversion arbeiten.

sicheres Browsen

Die meisten Hackerangriffe gelangen über das Internet auf Rechner und in Unternehmensnetzwerke. Damit es für Mitarbeiter möglich ist, sicher zu surfen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam mit dem IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity den R&S®Browser in the Box entwickelt. Der Nutzer arbeitet darin mit einer vom Betriebssystem separierten Maschine. Er bewegt sich sozusagen in einer virtuellen „Surfumgebung". Der Vorteil: Anstatt – wie bei Antivirenprogrammen – Schadcodes zu erkennen, werden alle potenziell gefährlichen Aktivitäten in diesem virtuellen Browser isoliert. Jeder Browserstart beseitigt die Schädlinge und versetzt den Browser in seinen Ausgangszustand. Die konsequenteste Netzwerktrennung erreicht man mit einer vollvirtualisierten Surfumgebung.
Weitere Informationen: **http://rohde-schwarz.com/cybersecurity/browser-in-the-box**

sichere Passwörter

Passwörter schützen die digitale Infrastruktur eines Unternehmens vor dem Zugriff unbefugter Personen. Je stärker ein Passwort ist, desto besser ist sein Schutz. Gute Passwörter sind beispielsweise so genannte Passphrasen, wie „Wir verschlüsseln Datenträger!" oder „keine-Zellen-in-Excel-verbinden". Solche Sätze sind leicht zu merken und zu tippen, aber schwierig zu knacken. Ergänzt werden sollten sie um Symbole, Zahlen oder Großbuchstaben.

Jede Anwendung sollte mit einem eigenen Passwort geschützt werden. Andernfalls muss ein Angreifer lediglich eine Anwendung erfolgreich kompromittieren, um sich bei weiteren Konten erfolgreich anzumelden. Auf haveibeenpwned.com kann man übrigens überprüfen, ob dies bereits geschehen ist.

Um nicht den Überblick zu verlieren, ist es hilfreich, einen Passwort-Manager zu nutzen. Das Programm speichert die Passwörter in einer Art Tresor – im Bedarfsfall kann man sie dort leicht wieder abrufen. Einen Passwortmanager schützt man am besten mit einer starken Passphrase sowie einer zweistufigen Verifizierung.

7. Vorsicht vor Betrügern. Angreifer täuschen und tricksen, um an Passwörter, Bankverbindungen oder Zugangsinformationen zu gelangen. Beispielsweise versenden sie täuschend echt wirkende E-Mails. Neben Phishing gilt aber auch Vorsicht bei Anrufen, SMS, Social-Media-Inhalten und gefälschten Nachrichten, die über Messenger verbreitet werden. Dieses sogenannte Social Engineering stellt in Zeiten dramatischer Veränderungen eines der größten Risiken im Home Office dar.

8. Unternehmen sollten sichere Kommunikationskanäle nutzen, um die Tablets, Smartphones oder PCs der Mitarbeiter im Home Office an das Unternehmensnetzwerk anzubinden. Empfehlenswert sind Virtual Private Networks (VPN). Sie bauen über einen „gesicherten Tunnel" Verbindungen zwischen dem Endgerät und dem Unternehmensnetz auf.

9. Starke Passwörter nutzen. Passwörter schützen Anwendungen vor unberechtigtem Zugriff. Je komplexer und eindeutiger Passwörter sind, desto schwerer sind sie zu knacken. Eine Multi-Faktor-Authentifizierung beispielsweise unter Einsatz von PIN, Fingerabdruck oder Passwort bietet ergänzend Schutz vor dem Zugriff unbefugter Dritter. Mehr dazu im Infokasten „Sichere Passwörter".

10. Daten in der Cloud schützen. Für das dezentrale Arbeiten sind Cloud-Anwendungen und Collaboration-Dienste ideal. Doch die Schutzmechanismen der Cloud-Anbieter entsprechen meist nicht den Sicherheitsanforderungen vieler Unternehmen. Es drohen Datenspionage und Compliance-Verletzungen. Die Lösung ist ein datenzentrischer Schutz: Dabei werden Platzhalter in die Cloud eingestellt, die nur Metadaten enthalten, die für Kollaboration und Workflows notwendig sind. Die schützenswerten Nutzdaten werden fragmentiert im Unternehmensnetzwerk oder an einem anderen Ort abgelegt.

Autor: Dr. Falk Herrmann, CEO von Rohde & Schwarz Cybersecurity
www.rohde-schwarz.com/cybersecurity

Nachruf

Mit tiefer Trauer und Bestürzung teilen wir mit, dass

Dr. Carl Dujat

einer der in Deutschland engagiertesten Medizininformatiker im Alter von 56 Jahren überraschend und viel zu früh verstorben ist.

Dr. Dujat war für uns ein toller, warmherziger Kollege mit exzellenter Expertise. Er studierte in Heidelberg Medizinische Informatik, arbeitete danach am Universitätsklinikum Heidelberg, wo er das Zentralarchiv mit aufbaute. Danach übernahm er am Universitätsklinikum Aachen die Leitung des Zentralarchivs, das er modernisierte und auf eine informatik-gestützte Verwaltung umstellte.

1997 war er Mitbegründer und später Vorstandsvorsitzender der promedtheus AG, einem renommierten Unternehmen für die IT-Beratung im Gesundheitswesen.

Schon 1993 war er Mitbegründer der GMDS-Arbeitsgruppe "Archivierung von Krankenunterlagen", in der er sich in leitender Funktion bis heute engagierte.
Von 2008 -2013 war er Präsident des Berufsverbandes Medizinischer Informatiker, dessen erweiterter Vorstand am 14.02.2020 beschlossen hatte, Dr. Dujat die Ehrenpräsidentschaft des Verbandes zu verleihen. Eine entsprechende Auszeichnung erfolgt nun leider nur noch im würdigen Rahmen posthum.

Er baute maßgeblich den conhIT-Kongress als Vorläufer der DEMA mit auf, für den er von 2009 – 2012 mit Kongresspräsident war.

2006 war er Mitbegründer der ENTSCHEIDERFABRIK und bis zuletzt Stv. Vorsitzender des Lenkungskreises des wirtschaftlichen Geschäftsbetriebs und Vice President HIE des VuiG e.V.

Ferner war er maßgeblich an der Gründung des CCESigG beteiligt.

Neben allen Aktivitäten setzte er sich für die Medizinische Informatik in verschiedensten Funktionen und für sachgerechte Lösungen in der Patientenversorgung ein. Auch organisierte er fortwährend mit Fachkolleginnen und -kollegen wertvolle Veranstaltungen für die Branche.

Dr. Dujat hinterlässt eine große Lücke für uns. Er wird uns immer in bester Erinnerung sein.
Mit unseren Gedanken sind wir bei seiner Familie.

Verband der Krankenhausdirektoren Deutschlands e.V.

TMF

GuiG IuiG VuiG ENTSCHEIDERFABRIK

bdvb Das Netzwerk für Ökonomen

bvitg Bundesverband Gesundheits-IT

BVMed Gesundheit gestalten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

BVMI Berufsverband Medizinischer Informatiker e.V.

IHE DEUTSCHLAND Integrating the Healthcare Enterprise

HL7 Deutschland

CCESigG

SEIT 1997 promedtheus Informationssysteme für die Medizin AG

CeMPEG

AHIME Association of Health Information Management Executives

Wir haben Carl vor vielen Jahren kennen gelernt und als Freund geachtet und geschätzt. Nachdem wir uns selbständig gemacht hatten, hat er sich als Kooperationspartner angeboten; damit kamen große gegenseitige berufliche Respektierung und Wertschätzung hinzu.

Wir waren zwar nicht immer einer Meinung, aber wir fanden immer eine gemeinsame Basis und Konsens für die vielen gemeinsamen sowie sehr erfolgreichen Projekte.

Wir vermissen Carl sehr und werden ihn stets in ehrender Erinnerung behalten.

Cornelia Vosseler und Hans-Werner Rübel

In unserer Branche haben wir uns vor vielen Jahren in gemeinsamen Projekten kennengelernt, lieber Carl. Fußball und Golf standen bei unseren privaten Treffen im Vordergrund.

Wir behalten Dich so in Erinnerung wie auf diesem Bild - voller Lebenslust und Freude.
Dr. Pierre-Michael Meier, Dr. Aykut M. Uslu, Kai de Fries

CLOVERLEAF®

Der Kommunikationsserver

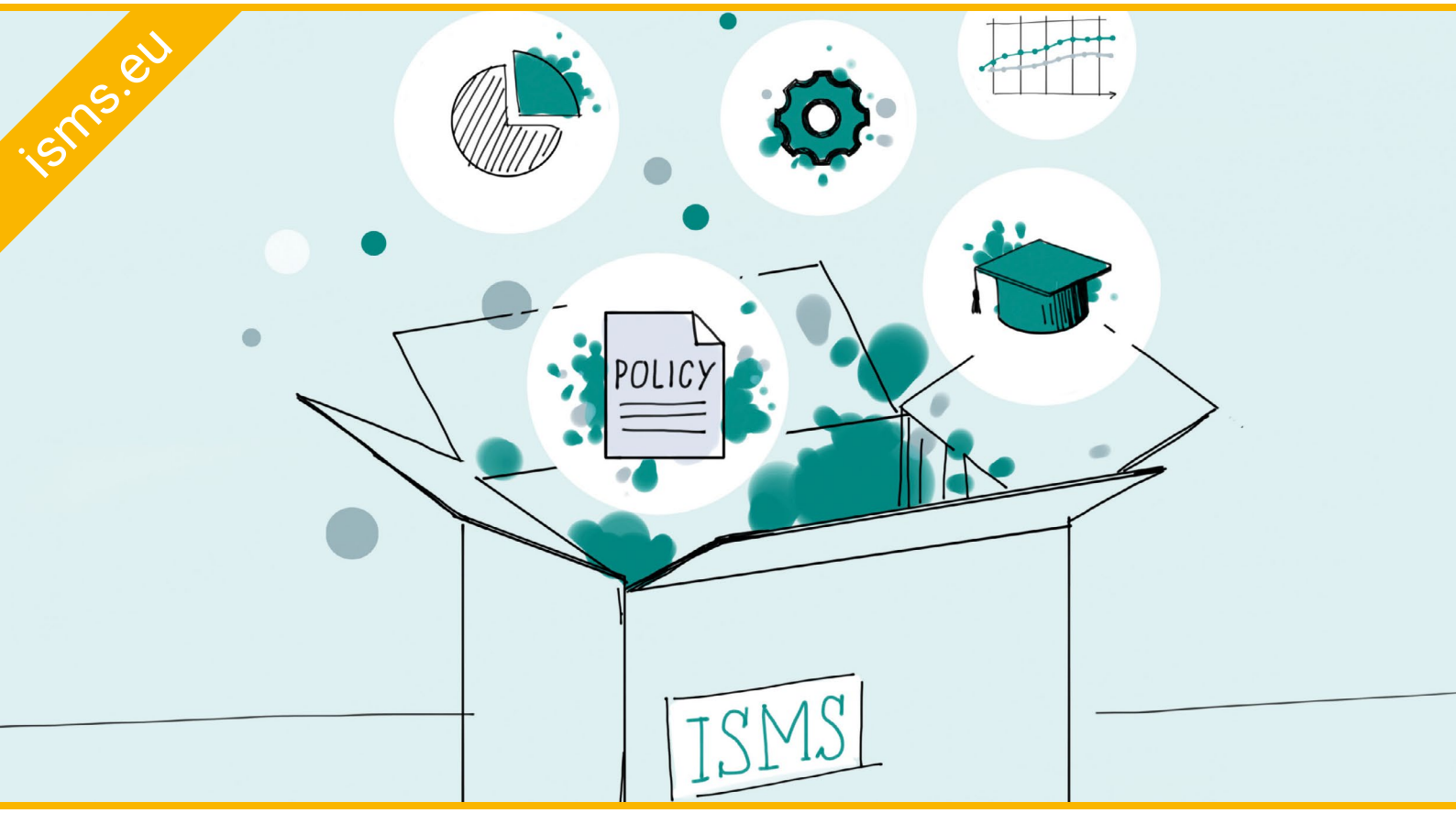
Intelligente Verbindungen.
Auf höchstem Niveau.

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

ISMS

In zwei Schritten zum ISMS.



Das ISMS Vorlagen-Komplettpaket nach ISO 27001 und B3S

Unsere Spezialisten unterstützen Sie bei der Einführung eines Informationssicherheits-Managementsystems (ISMS) und stellen Ihnen ein umfangreiches Vorlagen-Komplettpaket für Richtlinien, Prozessbeschreibungen und andere notwendige Dokumente bereit. **Mehr dazu auf www.isms.eu.**

Schritt 1 → Vorlagen befüllen

Schritt 2 → ISMS einführen

Ihre Vorteile

- Erfahrungswerte aus über 10 Jahren zertifiziertem ISMS-Betrieb
- Textbausteine und Inhalte sind umfassend vorformuliert und kommentiert
- Unsere Experten beraten mit fundiertem Know-how aus dem Gesundheits- und Sozialwesen
- Deutliche Zeitersparnis und Aufwandsreduktion beim ISMS-Aufbau
- Perfekte Basis für eine ISO/IEC 27001-Zertifizierung und einen erfolgreichen Nachweis gemäß §8a BSIG
- Keine Spezialsoftware notwendig – Sie benötigen nur Microsoft Office

Ihr Ansprechpartner:

Michael Punz
CISO und Geschäftsbereichsleiter
Datenschutz & Informationssicherheit
+43 7242 2155-6325 | michael.punz@x-tention.at