IT-Sicherheitsgesetz: Melde- und Nachweispflicht für Kritis-Betreiber entscheidend

Der Countdown läuft

Mit der 2014 verabschiedeten Digitalen Agenda will die deutsche Bundesregierung den digitalen Wandel aktiv begleiten und mitgestalten, um die Zukunftsfähigkeit des Landes zu sichern. Ein wichtiger Baustein ist das am 25. Juli 2015 in Kraft getretene IT-Sicherheitsgesetz, das die gesetzlich verbindliche Etablierung eines Mindestniveaus an IT-Sicherheit zum Gegenstand hat. Ein Dokumentenmanagementsystem beispielsweise bietet rechtskonforme Dokumentenvorlagen und erlaubt die recht- und zweckmäßige Verarbeitung persönlicher Daten.

Matthias Kunisch, Geschäftsführer der forcont business technology GmbH: „Kritis-Betreiber müssen als Mindeststandard ein Informations-Sicherheits-Management-System einführen, mit dem sie Sicherheitsrisiken und IT-Störungen überwachen, bewerten, steuern und melden können." Bild: forcont

Vom IT-Sicherheitsgesetz betroffen sind Unternehmen aus den Sektoren Energie, Wasser, Informationstechnik, Telekommunikation, Ernährung, Finanzen, Transport, Verkehr und Gesundheit, die kritische Infrastrukturen, sogenannte Kritis, betreiben. Die Umsetzung des Gesetzes erfolgt in zwei Phasen: Zunächst sind nur Kritis-Betreiber aus den Bereichen ITK, Energie, Wasser und Ernährung betroffen, die anderen ziehen später nach.

Seit Mai 2016 hatten die Betroffenen sechs Monate Zeit, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Kontaktstelle für Vorfallsmeldungen zu nennen. Zudem müssen sie ihre IT bis Mai 2018 nach dem Stand der Technik absichern, etwa nach nationalen oder internationalen DIN- oder ISO-Standards. Schließlich hätten Versorgungsengpässe oder gar komplette Systemausfälle dramatische Folgen – sowohl für die Verbraucher als auch für die Wirtschaft und den Staat.

Mit einem Dokumentenmanagementsystem lassen sich Projekte wie die IT-Sicherheit besser managen. Im Falle eines Cyber-Angriffs lässt sich damit dokumentieren, wie die Sicherheitsstrategie umgesetzt wurde. Bild: Sergey Nivens, shutterstock.com

Ein Informations-Sicherheits-Management-System muss sein

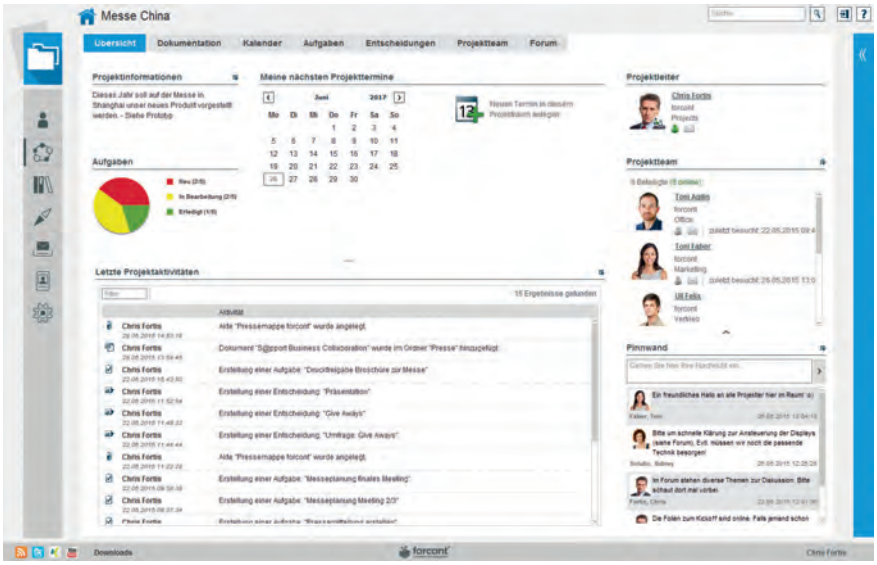
Mit dem Gesetz zur Steigerung der Sicherheit informationstechnischer Systeme gehen neue Pflichten zur Erhöhung von Abwehrmaßnahmen sowie Nachweis- und Meldepflichten einher. Zudem müssen Kritis-Betreiber als Mindeststandard ein Informations-Sicherheits-Management-System (ISMS) einführen, mit dem sie Sicherheitsrisiken und IT-Störungen überwachen, bewerten, steuern und melden können. Hierfür sind:

- ein Nutzstrukturplan zu erstellen, der die schutzbedürftigen Komponenten des eigenen Netzes im Prozessumfeld mit den anzutreffenden Haupttechnologien und Schnittstellen umfasst;
- eine Schutzbedarfsanalyse durchzuführen, die die Ziele der Informationssicherheit berücksichtigt (Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit);
- ein IT-Sicherheitsbeauftragter zu bestellen, der die Koordination, Verwaltung und Kommunikation der Informationssicherheit übernimmt;
- ein Zertifikat zu erwerben, das die Konformität des ISMS mit der Norm ISO/IEC 27001 bestätigt.

Transparente Dokumentation der Maßnahmen

Mit der bloßen Einführung eines ISMS ist es aber nicht getan. Ebenso wichtig ist die Dokumentation vorgenommener sicherheitsrelevanter Anpassungen. Ohne eine transparente Dokumentation laufen Unternehmen Gefahr, gegen Compliance-Richtlinien zu verstoßen. Sie müssen jederzeit nachweisen können, dass sie sich mit den erforderlichen Maßnahmen zum Management von IT-Risiken auseinandergesetzt und die

verbindlichen Vorgaben des IT-Sicherheitskatalogs umgesetzt haben. Auch für den Fall eines Cyberangriffs ist sauber zu dokumentieren, dass die betroffenen IT-Systeme gemäß IT-Sicherheitsgesetz aufgestellt sowie geschützt sind und das BSI über den Vorfall korrekt informiert wurde. Sind Betreiber von Kritis dazu nicht in der Lage, drohen Bußgelder in Höhe von bis zu 100.000 Euro.
Am einfachsten kommen Unternehmen der Dokumentationspflicht mit einem professionellen Dokumentenmanagementsystem (DMS) nach. Es leistet insbesondere in drei Bereichen, die unmittelbar mit der Umsetzung der Vorgaben des IT-Sicherheitsgesetzes verknüpft sind, wertvolle Unterstützung: bei der Erstellung, Verbreitung und Archivierung von Dokumenten.



Ein DMS lässt sich konfigurieren und damit an den eigenen Workflow, die Sicherheitsroutinen sowie die Bediener- und Mitarbeiterrechte anpassen. Bild: forcont

Dokumente direkt im DMS erstellen

Allein bei der Einführung des ISMS und bei der Erarbeitung des Netzstrukturplans entstehen Unmengen verschiedener Dokumente: Anforderungsanalysen, Lastenhefte, Zeitpläne, Protokolle, Technologie-, Prozess- und Schnittstellenbeschreibungen etc. Ohne ein DMS müssen Unternehmen die benötigten Dokumente am PC erstellen, bearbeiten, finalisieren, ausdrucken, gegebenenfalls unterschreiben lassen und versenden sowie in einer Akte ablegen, einscannen oder digital ablegen – ein höchst zeitraubendes und zugleich fehleranfälliges Vorgehen.

Die IT-Systeme müssen geschützt werden. Im Falle von Cyber-Angriffen muss die eigene Organisation so aufgestellt sein, dass das Bundesamt für Sicherheit in der Informationstechnik umgehend und ausführlich darüber informiert wird. Bild: stevepb, pixabay.com

Wesentlich effizienter ist eine integrierte Dokumentenerstellung: Die Mitarbeiter fertigen die benötigten Dokumente direkt im DMS an – etwa innerhalb einer Vorgangsbeschreibung – speichern sie an selbiger Stelle und versenden sie bei Bedarf direkt aus dem System heraus per E-Mail an einen Adressaten wie das BSI oder die Zertifizierungsstelle. Weiterhin sichert ein DMS die Aktualität der Dokumente, indem sich Wiedervorlagen zur Überprüfung individuell einstellen lassen. So müssen Kritis-Betreiber nicht nur ihre IT-Systeme in definierten Zeiteinheiten überprüfen, sondern auch die Menschen, die damit arbeiten.
Insbesondere international tätige Unternehmen sind verpflichtet, die persönlichen Daten ihrer Beschäftigten regelmäßig gegen die EU-Anti-Terror-Verordnungen oder Sanktionslisten (EU-Verordnungen) abzugleichen. Auch hier sorgt ein DMS für die nötige Transparenz: Es zeigt auf, welcher Mitarbeiter wann kontrolliert wurde und wo die entsprechenden Dokumente hinterlegt sind.

Compliance-Richtlinien erfüllen

Selbstverständlich ist insbesondere bei gesetzlichen Vorgaben, wie sie das IT-Sicherheitsgesetz macht, unbedingt auf die Compliance zu achten. Um auf der sicheren Seite zu sein, müssen Kritis-Betreiber gewährleisten können, dass nicht nur Entwürfe und nachträgliche Veränderungen von Dokumenten vollständig dokumentiert und jederzeit nachvollziehbar sind, sondern auch die Mitarbeiter, die diese erstellt oder verändert haben. Denn üblicherweise sind an der Dokumentenerstellung viele Mitarbeiter aus verschiedenen Unternehmensbereichen beteiligt. Ein DMS speichert sämtliche Versionen eines Dokuments samt Metadaten in der Historie – von der Bearbeitungszeit über den ausführenden Mitarbeiter bis hin zu den eigentlichen Änderungen.

Datenschutzbestimmungen einhalten

Beinhaltet ein Dokument persönliche Daten, sind die geltenden Datenschutzbestimmungen einzuhalten: Der Betroffene muss der Erhebung und Verarbeitung seiner personenbezogenen Daten zustimmen – zumal Unternehmen jene Daten nur zweckgebunden verarbeiten dürfen. Ein DMS bietet rechtskonforme Dokumentenvorlagen und erlaubt die recht- und zweckmäßige Verarbeitung persönlicher Daten, da sich bestimmte Felder voreinstellen lassen. Darüber hinaus dürfen Dokumente nicht allen Mitarbeitern zugänglich sein, sondern nur jenen, die sie benötigen, um eine bestimmte Aufgabe zu erfüllen.
Über ein Berechtigungssystem lässt sich festlegen, welche Personen oder Personengruppen auf welche Dokumente wie lange zugreifen dürfen – von bloßen Leserechten bis hin zu Bearbeitungs- oder Freigabebefugnissen.
Ein wesentlicher Vorteil eines DMS ist, dass Unternehmen Dokumente samt relevanten Unterlagen direkt aus dem System heraus per E-Mail verschicken können. Insbesondere im Falle von Cyber-Attacken oder IT-Störungen ist das fundamental wichtig. Damit der integrierte E-Mail-Versand auch während eines Angriffs funktioniert, sollten Kritis-Betreiber das DMS in einer geschützten Umgebung offline betreiben: in ihrem eigenen Rechenzentrum und Netzwerk. Nur dann können sie Sanktionen entgehen und ihrer Pflicht nachkommen, erhebliche Störungen ihrer IT zu melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können. Adressat der Meldung ist das BSI als zentrale Melde- und Aufsichtsstelle. Das DMS sorgt für einen funktionierenden Workflow, indem der verantwortliche Mitarbeiter per Mausklick alle Informationen zur Störung oder zum Angriff an das BSI übermitteln kann. Die aus der Meldung gewonnenen Erkenntnisse stellt das BSI sowohl den übrigen Kritis-Betreibern als auch den zuständigen (Aufsichts-)Behörden zur Verfügung, sodass diese ihre IT-Systeme adäquat schützen und entsprechende Maßnahmen einleiten können.
Auch bei der Erfüllung der Meldepflicht ist die Compliance sehr wichtig: Über das DMS können Unternehmen transparent nachweisen, dass sie sich korrekt verhalten und welche Maßnahmen sie eingeleitet haben, um zukünftigen Störungen oder Cyber-Attacken vorzubeugen.

DMS unterstützt (Re-)Zertifizierung

Mit dem Erwerb eines Zertifikats können Kritis-Betreiber die Wirksamkeit und Normenkonformität ihrer IT-Systeme nachweisen und dokumentieren, dass sie die Vorgaben des IT-Sicherheitskatalogs umgesetzt und eingehalten haben. Die Zertifizierung ist zwei Jahre gültig und erfordert eine Re-Zertifizierung durch eine akkreditierte Zertifizierungsstelle.
Um diesen Termin nicht zu versäumen, verfügt ein DMS über eine Fristenkontrolle: Zu einem definierten Zeitpunkt vor dem Ablaufdatum erhält der zuständige Mitarbeiter eine Erinnerung per E-Mail, sodass er die Re-Zertifizierung in die Wege leiten kann. Lässt er die Frist verstreichen, wird diese automatisch an den Nebenverantwortlichen weitergeleitet.
Auch bei der eigentlichen Zertifizierung leistet ein DMS praktische Unterstützung. Der Verantwortliche erstellt definierte Aufgabenlisten und weist sie den entsprechenden Kollegen zu. Nach Erfüllung der Aufgabe markieren diese die Tasks als ‚erledigt' und speichern sie samt abgearbeiteter Aufgabenliste in

der Dokumentation. So kann erreicht werden, dass alle für die Re-Zertifizierung benötigten Dokumente rechtzeitig vorbereitet und zusammengestellt sind.

Nachweispflicht: Dokumente langzeitig archivieren

Die Nachweispflicht ist ein zentraler Aspekt des IT-Sicherheitsgesetzes. Kritis-Betreiber müssen mittels Zertifizierung gegenüber dem BSI alle zwei Jahre nachweisen, dass ihre IT-Systeme dem Stand der Technik entsprechen. Ein DMS bietet umfassende Möglichkeit zur Langzeitarchivierung von Dokumenten aller Art: vom Netzstrukturplan und der Schutzbedarfsanalyse über Datenschutzhandbücher und Informationen zum IT-Sicherheitsbeauftragten bis hin zu Zertifikaten, Qualitätssicherungsnachweisen und Vorfallsmeldungen.
Da Anwender die Dokumente mit aussagekräftigen Tags und Metadaten versehen können, sind sie später schneller und unkompliziert auffindbar. Eine hohe Sicherheit gewähren bedarfsgerecht wählbare Sicherheitsstufen für die Dateiablage.
Auch bei der Archivierung ist auf den Schutz personenbezogener Daten zu achten, etwa mittels Pseudonymisierung und Verschlüsselung.
Obwohl Unternehmen personenbezogene Daten prinzipiell nur so lange speichern dürfen, wie für die Erfüllung des verbundenen Zwecks nötig ist, gibt es Ausnahmen, wie etwa Archivierungszwecke. In einem DMS lassen sich automatisierte Workflows zur Prüfung der jeweiligen Zweckbindung anlegen. Sind die nötigen Datenschutz-Anforderungen erfüllt, dient die Langzeitarchivierung als Grundlage für die Erstellung detaillierter Analysen und aussagekräftiger Auswertungen: Wie viele Angriffe gab es? Wann ist eine Attacke geschehen? Welches Ausmaß hatte eine Störung? etc.
Daraus können Kritis-Betreiber wichtige Schlüsse für den zukünftigen Schutz ihrer IT ziehen – und sind zugleich rechtlich auf der sicheren Seite.

Matthias Kunisch

Kontakt

forcont business technology gmbh
Nonnenstraße 39
04229 Leipzig
Tel.: +49 341 48053-0
info@forcont.de
www.forcont.de

Studie: E-Health steigert nachhaltig die Effizienz im Gesundheitswesen

E-Health schafft Effizienzpotenziale

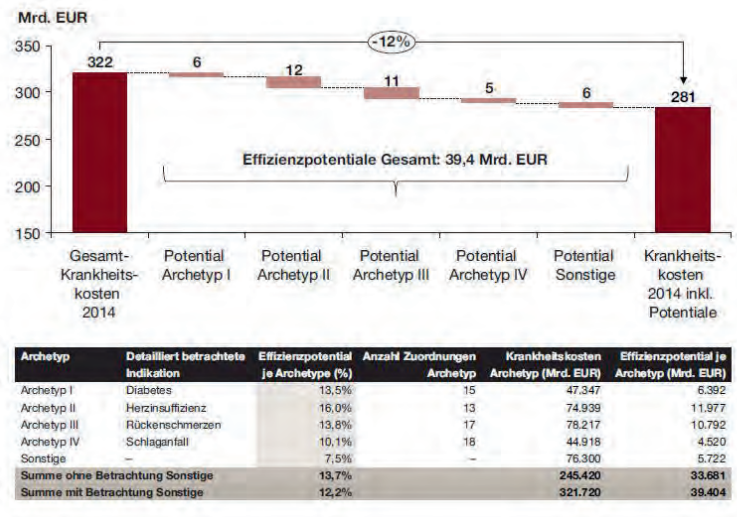
Trendcluster im Gesundheitswesen

Die Vernetzung des Gesundheitswesens ist unvermeidlich – das zeigt die Studie ‚Effizienzpotentiale durch E-Health', die von PwC Strategy& im Auftrag des Bundesverbands Gesundheits-IT e. V. (bvitg) und der CompuGroup Medical SE durchgeführt wurde. Erstmalig beziffert die Untersuchung das enorme wirtschaftliche Potenzial von E-Health-Lösungen und zeigt, dass eine Realisierung positiver Effekte durch E-Health in Deutschland ohne Einschränkungen der Versorgungsqualität der Patienten möglich ist.

In den kommenden Jahren steht das deutsche Gesundheitswesen vor erheblichen Herausforderungen und Veränderungen. Trotz des demografischen Wandels und der steigenden Gesundheitsausgaben muss die hohe Qualität der Gesundheitsversorgung der Bevölkerung weiterhin gewährleistet werden. Zudem verändern sich die Prozesse durch die zunehmende Digitalisierung in allen Bereichen der Gesellschaft, der Wirtschaft und der Verwaltung nachhaltig: mit dem Smartphone bezahlen, Buchungen auf Online-Portalen durchführen oder Videotelefonie gehören heute zum Alltag. Betrachtet man jedoch im Vergleich dazu das Gesundheitswesen, so stellt man fest, dass in der deutschen Gesundheitsversorgung eine vergleichbar hohe Adoptionsrate digitaler Anwendungen bisher ausgeblieben ist.

Produktivitätsparadoxon der IT

Wenn man grundsätzlich von Investitionen in Gesundheits-IT spricht, lautet die erste Frage häufig: Welchen Nutzen hat sie? Vor dem Hintergrund knapper Ressourcen ist die Kosten-Nutzen-Betrachtung von Investitionen in die IT eine berechtigte und häufig geforderte Entscheidungshilfe. Diese birgt jedoch nicht zu vernachlässigende methodische Problemfelder in sich. Bereits Mitte der 1990er Jahre wurde eine Vielzahl quantitativ orientierter empirischer Untersuchungen mit dem Ergebnis durchgeführt, dass insbesondere im Dienstleistungssektor kein explizit nachweisbarer Zusammenhang zwischen IT-Investitionen und der Steigerung der Produktivität besteht. Diese Ergebnisse beleben die als ‚Produktivitätsparadoxon der IT' geführte wissenschaftliche Diskussion bis heute.
Im Gesundheitswesen existieren einige Studien zur Debatte über den Wertbeitrag von IT – ohne jedoch den Anspruch an eine einheitliche wissenschaftliche Lehrmeinung zu erheben. So lag bis vor Kurzem auch keine Untersuchung vor, die auf Basis weiter gefasster Analysen und entlang medizinisch validierter Behandlungspfade das Effizienzpotenzial von E-Health umfänglich quantifiziert. Diesem Thema hat sich nun im Auftrag des Bundesverbands Gesundheits-IT e. V. (bvitg) und der CompuGroup Medical SE das Strategieberatungsteam von PwC angenommen.



Archetyp	Detailliert betrachtete Indikation	Effizienzpotential je Archetype (%)	Anzahl Zuordnungen Archetyp	Krankheitskosten Archetyp (Mrd. EUR)	Effizienzpotential je Archetyp (Mrd. EUR)
Archetyp I	Diabetes	13,5%	15	47.347	6.392
Archetyp II	Herzinsuffizienz	16,0%	13	74.939	11.977
Archetyp III	Rückenschmerzen	13,8%	17	78.217	10.792
Archetyp IV	Schlaganfall	10,1%	18	44.918	4.520
Sonstige	–	7,5%	–	76.300	5.722
Summe ohne Betrachtung Sonstige		13,7%		245.420	33.681
Summe mit Betrachtung Sonstige		12,2%		321.720	39.404

Extrapolation auf Basis der Studiengrundlage auf weitere Indikationsbereiche

Effizienzpotenzial liegt bei rund 39 Milliarden Euro

Ergebnis der Studie ‚Effizienzpotenziale durch E-Health' von Strategy& ist, dass die flächendeckende Einführung von E-Health-Lösungen weitreichende Potenziale bietet. Demnach lässt sich das durch deren konsequenten Einsatz im deutschen Gesundheitswesen realisierbare Effizienzpotenzial auf rund 39 Milliarden Euro beziffern, was ca. zwölf Prozent der gesamten GKV-Krankheitskosten in 2014 entspricht.
Zur Ermittlung dieser Summe berücksichtigte das Beratungsunternehmen von Ärzten validierte Annahmen vergleichbarer Indikationsbereiche sowie Erkenntnisse bestehender Primärstudien und konservativer Grundannahmen. Dementsprechend sind indirekte Krankheitskosten, wie beispielsweise Arbeitsunfähigkeit, nicht enthalten. Zusätzlich wurde Wert darauf gelegt, dass notwendige medizinische Behandlungen in vollem Umfang und leitliniengestützt erfolgen und damit negative Auswirkungen auf die Versorgungsqualität von Patienten ausgeschlossen sind.

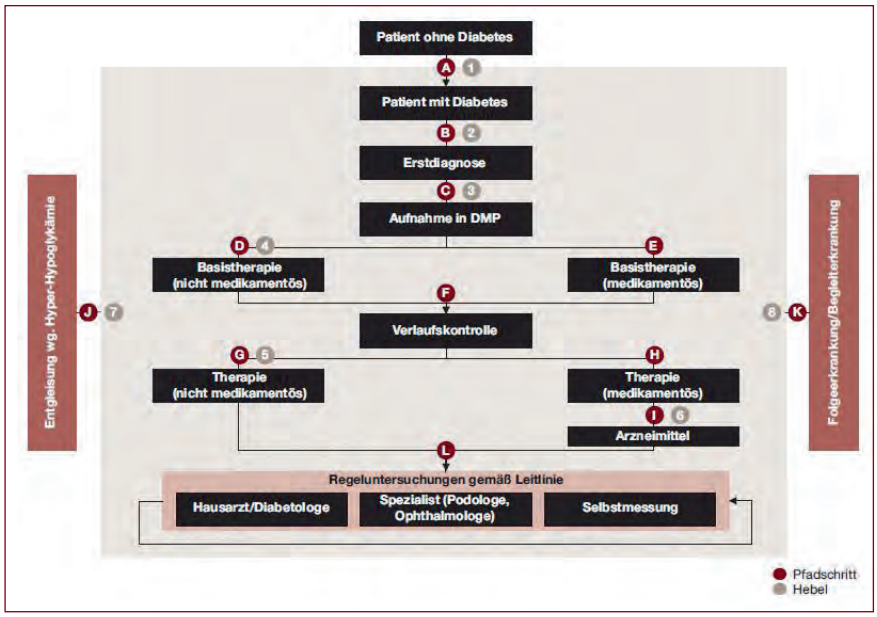
Potenzial von E-Health quantifizieren

„Die Studie zeigt die Relevanz digitaler Lösungen im Versorgungsalltag des deutschen Gesundheitssystems.

Schematische Darstellung der Bildung von Archetypen auf Basis detailliert betrachteter Indikationsbereiche

Die Einführung ist nur noch eine Frage des ‚Wann' und nicht mehr des ‚Ob'", erläutert Dr. Rainer Bernnat, Geschäftsführer von PwC Strategy& Deutschland. Uwe Eibich, Vorstand der CompuGroup Medical Deutschland AG, stellt zudem fest: „Die Potenziale von E-Health bleiben in Deutschland derzeit noch weitgehend ungenutzt. Die Kosten-Nutzen-Betrachtung von Investitionen in IT ist häufig eine geforderte Entscheidungshilfe. Mit dieser Studie ist es uns nun gelungen, die Potenziale von E-Health gesamtheitlich und erstmals anhand medizinisch validierter Behandlungspfade zu quantifizieren."
Dazu wurde ein Idealzustand (idealer Referenzrahmen) gedanklich vorausgesetzt. In diesem sind E-Health-Anwendungen bereits umfassend umgesetzt und in einer Gesamtlösung integriert.

Dabei zeigte sich, dass eine umfangreiche Digitalisierung der medizinischen Versorgung zu einer signifikanten Verbesserung sowohl der medizinischen als auch der prozessualen Exzellenz führt. Die detaillierte Betrachtung von vier archetypischen Indikationsbereichen (Diabetes, Herzinsuffizienz, Rückenschmerzen und Schlaganfall) belegt, dass E-Health beispielsweise Falsch-, Fehl- oder Doppelmedikationen (medizinische Exzellenz), aber auch Informationsverluste an Schnittstellen und Sektorengrenzen (operative Exzellenz) verhindern kann – und somit die Ärzte in ihrer Arbeit gezielt unterstützt.
So werden Leistungserbringer von nicht-medizinischen Routineaufgaben entlastet oder durch Expertensysteme in ihrer Arbeit unterstützt. Durch Nachuntersuchungen per Videotelefonie können zusätzlich



Behandlungspfad mit Effizienzhebeln

Bilder: Strategy & Analyse

Zeiträume zwischen Regeluntersuchungen bedarfsgerecht verlängert oder verkürzt und Patiententransporte vermieden werden. Zielgerichtete ambulante Versorgungsformen – insbesondere in ländlichen Regionen – werden so häufig erst möglich. Die dargestellten Ergebnisse untermauern insoweit die Chance, für die ärztliche Heilkunst dringend notwendige Ressourcen zu heben und somit einen Beitrag für die Herausforderungen der Zukunft zu leisten.

Arzt-Patienten-Dialog bleibt unersetzlich

„Wichtig ist zu betonen, dass die ärztliche Expertise und der damit einhergehende persönliche Arzt-Patienten-Dialog unersetzlich sind und bleiben. E-Health ist kein Ersatz, sondern unterstützt vielmehr aktiv bei der medizinischen Entscheidungsfindung und erleichtert die Implementierung sektorenübergreifender und multidisziplinärer Versorgungsmodelle“, erklärt bvitg-Geschäftsführer Sebastian Zilch.
Neben der Darstellung der Effizienzpotenziale durch E-Health beabsichtigte die Studie auch, den aktuellen Status und entsprechende Kritikpunkte in der E-Health-Diskussion – insbesondere vor dem Hintergrund der letzten ‚Gerüchte‘ rund um die elektronische Gesundheitskarte – aufzugreifen, fortzuentwickeln und erste Lösungsansätze bereitzustellen.
„Zur Realisierung der quantifizierten Potenziale sind strategische Entscheidungen von Stakeholdern und der Politik unabdingbar“, hält Uwe Eibich fest. „So kristallisierten sich aus der Summe der vorliegenden Analysen sowie nach Ansicht der im Rahmen dieser Studie befragten Akteure fünf prioritäre Handlungsfelder heraus.“
Diese Handlungsfelder umfassen zum einen die Entwicklung eines nationalen E-Health-Zielbilds zur Systematisierung wesentlicher Anwendungsbereiche. Zeitgleich ist der Aufbau einer sicheren Kommunikationsinfrastruktur im Gesundheitswesen essentiell. Zur Stärkung der Telematikinfrastruktur gilt es dabei, offene Schnittstellen zur Integration von Anwendungen aus dem weniger regulierten ‚Zweiten Gesundheitsmarkt‘ zu entwickeln, um den bereits heute häufig weit fortgeschrittenen Versorgungslösungen einen struk ‚turierten Einsatzrahmen zu geben.
Als dritte Handlungsempfehlung ergibt sich der frühzeitige und breitflächige Einsatz einer elektronischen persönlichen Patientenakte. Erst eine für den Patienten jederzeit zugängliche Akte kann seine informationelle Selbstbestimmtheit sichern und damit den verantwortungsvollen Umgang und Austausch von Gesundheitsdaten zwischen Patient und Arzt fördern.
Die Möglichkeit zur selektiven Freigabe von Gesundheitsinformationen sowie zur orts- und zeitungebundenen Interaktion mit Leistungserbringern macht den Patienten zum Manager seiner eigenen Gesundheit und versetzt ihn in die Lage, ein neues Selbstverständnis zu entwickeln. Zur Sicherstellung der Nutzungsbereitschaft ist zudem der Aufbau von ‚Digital Health Literacy‘ sowohl für das medizinische Fachpersonal als auch in der Bevölkerung anzustreben.

Schneller Transfer aus der Forschung zur Breitenanwendung

Schließlich setzt die Umsetzung technisch komplexer Lösungen mit hohen Sicherheits- und Funktionsanforderungen eine starke Gesundheitswirtschaft in Deutschland voraus. Um eine nachhaltige Innovationsfähigkeit in Deutschland zu erreichen, ist der schnelle Transfer vom Forschungsvorhaben über Pilotprojekte in die Breitenanwendung zu fördern. Gleichfalls ist die Entwicklung eines Rahmens wünschenswert, der über adäquate Studiendesigns zur Wirksamkeit von E-Health-Anwendungen die besten Lösungen transparent macht.
„Vor dem Hintergrund der Bundestagswahl 2017 offenbart die Studie eine breite Palette an Handlungsfeldern für die kommende Legislaturperiode“, formuliert Sebastian Zilch seine Erwartungen an die Politik. So soll die vorgelegte Studie als Ausgangspunkt für weitere Diskussionen rund um E-Health dienen.
Die gesamte Studie kann unter www.bvitg.de/publikationen/ eingesehen werden.

Natalie Gladkov

Kontakt

bvitg e. V.
Bundesverband Gesundheits-IT
Friedrichstraße 200
10117 Berlin
Tel.: +49 30 2062258-20
info@bvitg.de
www.bvitg.de

Schnelltest soll Risiken und Kosten durch multiresistente Keime reduzieren

Schnell über MRSA Bescheid wissen

Vorteile des MRSA-Tests

- Ergebnis nach zwei Stunden
- Erfassung aller elf Subtypen von MRSA
- Ausschluss anderer Staphylokokken
- gute PPV- und NPV-Werte
- wenig Hands-on-Zeit bei der Analyse

Für Krankenhäuser und Pflegeheime sind multiresistente Keime ein erhebliches gesundheitliches und finanzielles Risiko. Ein neuer Schnelltest, der Ergebnisse schon in zwei statt wie bislang üblich in 24 bis 48 Stunden liefert, soll rasch Klarheit schaffen, ob ein Risikopatient wirklich positiv ist. Die Verbreitung von Keimen soll so schneller gestoppt und damit unnötige Kosten vermieden werden.

Das Bakterium Staphylococcus aureus ist weit verbreitet und besiedelt zum Beispiel die Haut und auch die Schleimhäute von Menschen und Tieren. Durch den vermehrten Einsatz hat diese Art eine Resistenz gegen viele Antibiotika entwickelt. Als Krankenhauskeim bekannt ist MRSA (Methicillin-resistenter Staphylococcus aureus) einer der weltweit bedeutendsten multiresistenten Erreger und bei weitem nicht nur in Krankenhäusern zu finden.
Eine Besiedlung mit MRSA bedeutet jedoch nicht direkt, dass eine Erkrankung vorliegt, es steigt aber das Risiko einer Infektion. Kliniken stehen also vor dem Problem, den Eintrag und die Verbreitung von MRSA zu verhindern und so die Patienten und das Personal zu schützen. Kosten und Nutzen müssen dabei im Verhältnis stehen und idealerweise sollten die Gesamtkosten für das MRSA-Management durch geeignete Maßnahmen sinken.

Protektive Maßnahmen kosten Geld

Gerade Risikogruppen werden in Screenings untersucht, um den MRSA-Status zu ermitteln. In den Niederlanden werden diesem Prozedere mitunter alle neu aufgenommenen Patienten unterzogen. Bis zum Vorliegen des Ergebnisses kann es allerdings einige Zeit dauern, wenn kulturelle Verfahren verwendet werden. Bis dahin werden Risikopatienten entweder isoliert und/oder Barriere-Maßnahmen ergriffen. Allerdings kosten Einmalkittel und andere protektive Maßnahmen Geld. Auch der Arbeitsaufwand zur Versorgung von Patienten mit Barriere- und Isolationsmaßnahmen ist höher und damit für die Klinik teurer. Die längere Verweildauer der Patienten treibt die Kosten zusätzlich in die Höhe. Ergo: Je schneller man weiß, welcher Patient positiv ist, desto besser. Es entstehen weniger Kosten und eine Ausbreitung in der Klinik kann effektiver verhindert werden.
Konventionelle Methoden benötigen 24 bis 48 Stunden, um zu einem Ergebnis zu kommen. Die von Q-Bioanalytic entwickelte Realtime-PCR-Test QuickBlue liefert innerhalb von weniger als zwei Stunden ein Ergebnis. Dadurch lässt sich auch ein besiedelter Patient, der vorher nicht als Risiko eingeschätzt wurde, schnell erkennen und die Zeit, in der er zur Verbreitung des Keims im Krankenhaus beitragen kann, schrumpft spürbar zusammen. Bisherige Kosten-Nutzen-Analysen haben gezeigt, dass PCR-Screenings effektiv sind, aber teuer sein können. Dies hat verschiedene Gründe: Zum einen haben die Tests eine Ungenauigkeit, sodass es falsche positive Ergebnisse geben kann. Dies führt zu unnötigen Maßnahmen. Außerdem waren die Tests in der ersten Zeit der PCR-Methoden noch vergleichsweise teuer.
Das Kosten-Nutzen-Verhältnis ist beim QuickBlue günstiger, bei gleichzeitiger höherer Genauigkeit. Kosten können eingespart werden durch:

- ein schnelles Einstellen von Barriere- und Isolationsmaßnahmen bei negativ getesteten Patienten,
- ein früheres Beenden arbeitsintensiver Pflegemaßnahmen bei negativ getesteten Risikopatienten,
- zeitige effektive Maßnahmen (Dekolonisierung) bei positiv getesteten Patienten,
- die Vermeidung nosokomialer Kolonisierung im Krankenhaus, dadurch kürzere Verweildauer der Patienten insgesamt,
- weniger Komplikationen bei OPs (schlecht heilende Wunden),
- die Vermeidung von Umsatzeinbrüchen und Imageverlust bei Ausbruchssituationen.

In der Hygienearbeit ist es wichtig, schnell zu wissen, welcher Patient mit MRSA-besiedelt ist. So kann er schnell einer Dekolonisierung zugeführt werden. Bild: Q-Bioanalytic

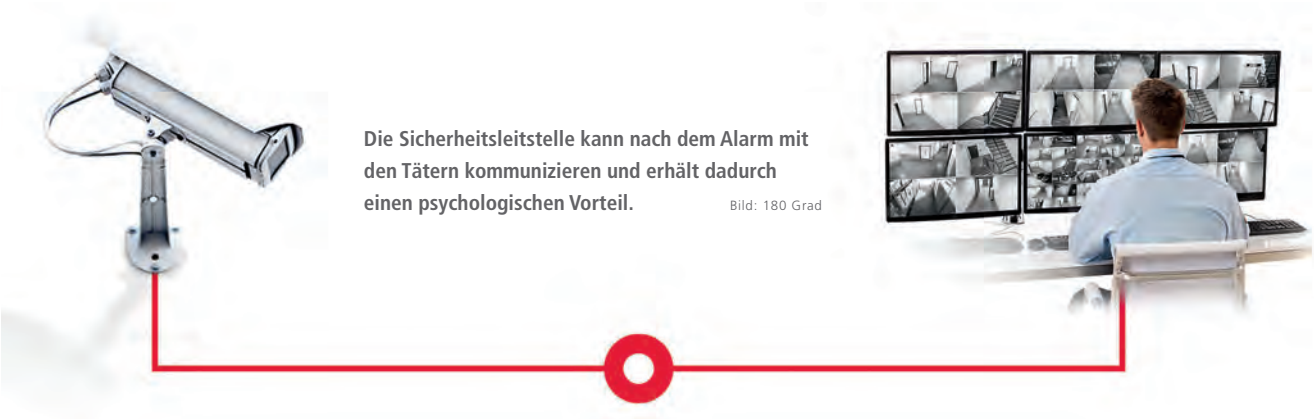
Dr. Boris Oberheitmann,
Dipl.-Biol. Kirsten Schönfeld

Kontakt

Q-Bioanalytic GmbH
Dr. Boris Oberheitmann
Fischkai 1
27572 Bremerhaven
Tel.: +49 471 900821-0
info@q-bioanalytic.com
www.q-bioanalytic.com

Live-Täteransprache für schnellen Kontakt zwischen Sicherheitspersonal und Täter

Smarter Diebstahlschutz



Die Sicherheitsleitstelle kann nach dem Alarm mit den Tätern kommunizieren und erhält dadurch einen psychologischen Vorteil. Bild: 180 Grad

Gut ausgeschilderte Krankenhausflure und einfach zugängliche medizinische Geräte: In Krankenhäusern wird es Dieben oft einfach gemacht. Smarte Sicherheitssysteme können hier helfen – und das sogar zweifach: Sie schrecken Täter ab und können zu spürbaren Einsparungen bei den Versicherungsprämien führen.

Es geschah am helllichten Tag in Pinneberg im Westen von Hamburg. Die Täter spazierten in die Regio-Kliniken und entwendeten hochwertige Medizintechnik. Nach ähnlichem Muster gingen sie auch in den städtischen Krankenhäusern in Kiel und Neumünster vor. Den ‚Rekord' hält das idyllische Ratzeburg mit fünf Besuchen in der dortigen Klinik. Seit 2016 verzeichnet das schleswig-holsteinische Innenministerium einen Gesamtschaden von etwa drei Millionen Euro.
Zuvor waren die Banden vornehmlich in Bayern und Nordrhein-Westfalen unterwegs. Aber auch Rheinland-Pfalz sieht sich einem wachsenden Interesse von Seiten der Diebe gegenüber. An drei Wochenenden hintereinander wurden in mindestens sechs Krankenhäusern im Südwesten Deutschlands teure Geräte gestohlen, darunter in fünf Kliniken in Rheinland-Pfalz und in einer im Saarland. Häufiges Ziel sind unter anderem endoskopische Systeme, insbesondere die Geräteköpfe, die sich bequem in Taschen transportieren lassen. Eine Aufklärungskampagne der Versicherer und der Krankenhausgesellschaften sollen das Personal sensibilisieren.

Effektiver Diebstahlschutz mit direktem Kontakt zu den Tätern

Herkömmliche Videoaufzeichnungen ermöglichen keine direkte Intervention, sondern nur eine Nachbetrachtung der Ereignisse. Dem gegenüber stehen Präventivmaßnahmen mithilfe moderner Elektrotechnik, zum Beispiel mithilfe einer elektronischen Zutrittskontrolle mit Diebstahlschutz und Live-Täteransprache. Dabei wird innerhalb von Sekunden nach Auslösung eines Alarms durch Bewegungsmelder eine Liveverbindung zwischen der VdS-zertifizierten Leitstelle des Sicherheitsunternehmens und dem betroffenen Raum oder Gelände hergestellt. Der Operator in der Leitstelle spricht den oder die Täter über eine Hör- und Sprechverbindung direkt an, eine Kamera behält diese im Blick. Zeitgleich informiert die Leitstelle die Polizei.
Der Vorteil des Diebstahlschutzes mit Live-Täteransprache gegenüber einer klassischen Alarmanlage ist die kurze Reaktionszeit. Der Datenschutz bleibt in allen anderen Situationen gewahrt, da eine Liveverbindung nur im Alarmfall aufgebaut wird. Kernelement der Abwehr von Dieben ist eine elektronische Zutrittskontrolle. Durch diese Kombination aus Zugangsmanagement und unmittelbarer Live-Täteransprache wird der Diebstahlschutz erst effektiv.

Daniel Althaus

Kontakt

180° Sicherheit GmbH
Hansaallee 321
40549 Düsseldorf
Tel.: +49 211 17607260
sicherheit@180-grad.de
www.180-grad.de