Verlagsbeilage, August 2014

‹kes›
Die Zeitschrift für Informations-Sicherheit

special

Initiative:
Datenschutz in der Arztpraxis
S. 18

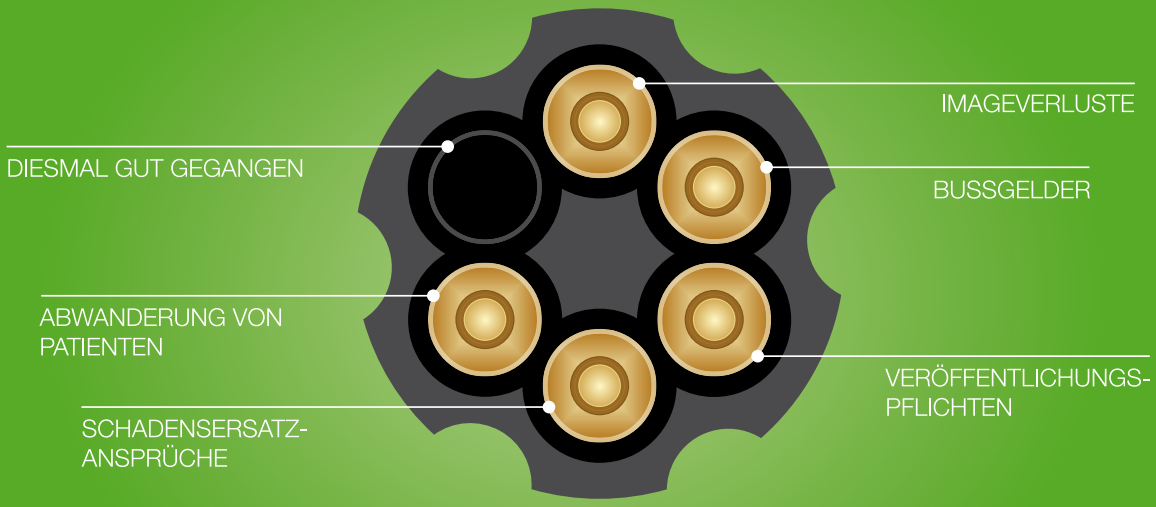
Software:
Praxissysteme schützen, Patientendaten sichern
S. 24

Datenschutz und IT-Sicherheit in Arztpraxis und Klinik

Risiko Mitarbeiter:
Insider-Threats in Klinik und Arztpraxis
S. 22

SecuMedia

E-Health: Der „Neue Markt" für Cyber-Kriminelle? ab S. 5



SPIELEN SIE KEIN **RUSSISCHES ROULETTE** MIT IHRER **EXISTENZ!**

SCHÜTZEN SIE DIE SENSIBLEN DATEN IHRER PATIENTEN!

Denn Patientendaten sind personenbezogene Daten und genießen daher besonderen Schutz.

EGOSECURE ENDPOINT

EFFEKTIV

EgoSecure Endpoint schützt effektiv vor allen Szenarien, die zu Datenverlusten führen können – insbesondere auch vor Datenverlusten durch unbeabsichtigte Fehler. Alle Anforderungen deutscher Gesetze und Regularien werden erfüllt.

EFFIZIENT

Die Installation von EgoSecure Endpoint ist einfach und schnell ohne externe Hilfe möglich. Die Administration ist intuitiv. Alle Schutzfunktionen finden im Hintergrund statt und stören die Mitarbeiter nicht bei ihrer normalen Arbeit.

Made in Germany

Schützen und managen Sie Ihre Patientendaten mit EgoSecure Endpoint.

Mehr Informationen und kostenlose Testlizenzen erhalten Sie unter:

patientendatenschutz.egosecure.com

EGOSECURE
ENJOY DATA PROTECTION

Zusammenwachsen der Technologien als Herausforderung für Datenschutz und Datensicherheit

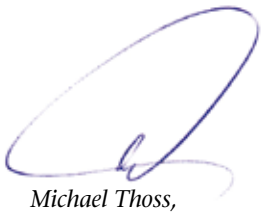
Vernetzung und die Integration von Technologien sind aktuelle Themen dieser Zeit. Ob dieses Ziel unter dem Oberbegriff der „Mobility“, „Cloud“ oder anderen Schlagworten behandelt wird, ist dabei unerheblich für die Herausforderungen im Bereich der Sicherheit und des Datenschutzes.

Die Verschmelzung der Kommunikationstechnik, Medizintechnik und Versorgungstechnik in Richtung „IP-Plattformen“ der Informationstechnik und der Ausbau der Telemedizin fordern die Kliniken in Deutschland in besonderem Maße heraus. Neben dem traditionell hohen Anspruch an den Schutz personenbezogener Daten, der intensiv und verantwortungsbewusst im Rahmen der eingesetzten Anwendungsverfahren gehandhabt wird, ergeben sich zusätzliche Herausforderungen durch Vernetzung und Integration einer Vielzahl weiterer technischer Systeme und der Bereitstellung dort erhobener Daten im Interesse der Versorgungs- und Behandlungsqualität des Patienten.

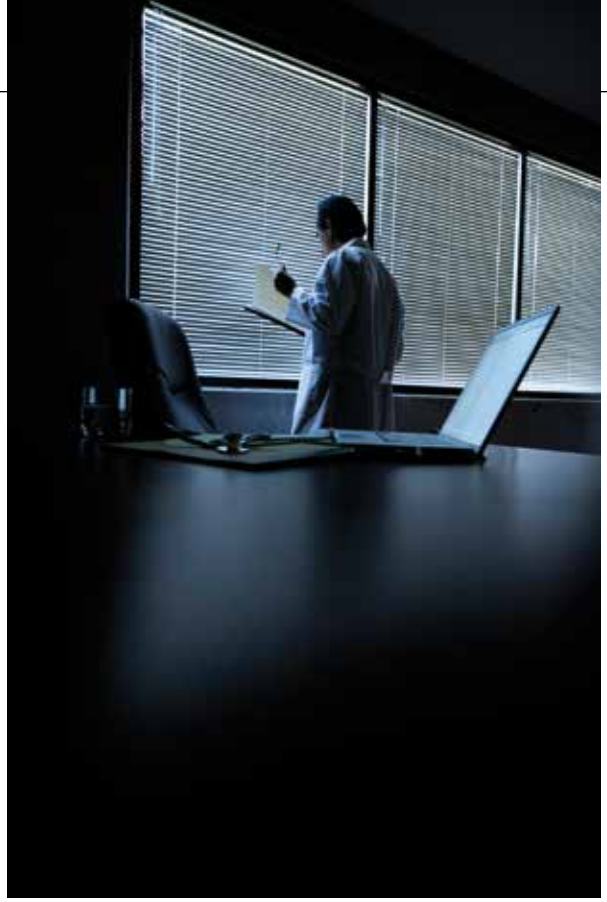
Gleichzeitig werden die gesammelten Daten im Interesse der reibungslosen Prozessgestaltung mobilisiert und treffen damit – theoretisch – auf eine fast unüberschaubare Anzahl weiterer potenzieller Strukturen und Endgeräte.

Dabei sind nicht alle „Betriebsmodelle“ mit den Anforderungen an die Sicherheit und den Datenschutz kompatibel. Begriffe wie „Cloud“, „Mobility“, „BYOD“ und andere werden schnell überreizt (hype) und halten den notwendigen Anforderungen an professionelle und sichere Strukturen nicht ohne Weiteres stand. Verschiedene, mit der Informationstechnologie verschmelzende Technologien, primär die Medizintechnik, zeichnen sich durch erheblichen Nachholbedarf bei der Sicherheit und Aktualität der eingesetzten Verfahren aus. Vormals „Insellösungen“ mit niedrigem bis keinem Gefährdungsgrad werden zunehmend in „vernetzte“ Strukturen integriert und bei ungenügender Härtung gegen Angriffe zum Sicherheitsrisiko. Darüber hinaus muss stets der Faktor Mensch durch Sensibilisierung, Schulung und Ausbildung auf Chancen und Risiken der Technologien hingewiesen werden.

Für Kliniken in Deutschland dominiert daher immer der Schutzgrad der verwalteten Daten vor der maximalen technologischen Verfügbarkeit. Die Sicherheit der den Krankenhäusern anvertrauten Daten hat die oberste Priorität und erfordert manchmal auch Verzicht aus Verantwortung.



Michael Thoss,
Vorstandsmitglied, Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V.



Impressum

SecuMedia Verlags-GmbH

Postanschrift: Postfach 12 34, 55205 Ingelheim (DE)
Hausanschrift: Lise-Meitner-Straße 4, 55435 Gau-Algesheim (DE)
Telefon +49 6725 9304-0, Fax +49 6725 5994
E-Mail: info@secumedia.de,
Web: www.secumedia.de

Beteiligungsverhältnisse
(Angabe gem. § 9, Abs. 4 Landesmedienges. RLP):
Gesellschafter zu je 1/6 sind Gerlinde Hohl, Klaus-Peter Hohl, Peter Hohl (GF),Veronika Laufersweiler, Nina Malchus (GF), Steffi Petersen

Handelsregister AG Mainz HRB 22282

Herausgeber: Peter Hohl

Redaktion: Oliver Schonschek (verantw. für den red. Teil)

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel. +49 6725 9304-20, E-Mail: anzeigenleitung@secumedia.de

Satz: BlackArt Werbestudio,
Stromberger Straße 47, 55413 Weiler bei Bingen

Druck: Schmidt printmedien GmbH
Haagweg 44, 65462 Ginsheim-Gustavsburg

Bildnachweis Titelbild, Seite 4: ©iStock.com/DNY59

Telematik-Infrastruktur schützt sensible Gesundheitsdaten

E-Health – Der „Neue Markt" für Cyberkriminelle?

Versorgungsqualität erhöhen und gleichzeitig Kosten senken – beides erfordert auch im Gesundheitswesen eine weitere Vernetzung von IT-Systemen und Softwarelösungen sowie die Automatisierung von Arbeitsprozessen über Systemgrenzen hinweg. Dies ruft aber auch ungebetene Akteure auf den Plan: Informationen aus dem Gesundheitssystem bringen bares Geld – nicht nur im Fall der gestohlenen Krankenakte eines mehrfachen Formel-1-Weltmeisters.

Von Wilfrid Kettler, GAI NetConsult GmbH

„Diebstahl aus Klinik: Schumacher-Akte stand zum Verkauf", „Patientendaten der Krankenkassen können per Telefon abgefragt werden", „ICS-CERT warnt: medizinische Geräte haben feste / bekannte Passwörter" – solche und ähnliche Hinweise auf Datenschutzverletzungen im Gesundheitswesen ereilen uns nahezu täglich. Bei immer mehr elektronisch gespeicherten medizinischen Daten und zunehmendem Datenaustausch müssen wir wohl zukünftig mit noch mehr solchen Alarmmeldungen rechnen.

Die Ausgaben im Gesundheitsmarkt umfassten schon 2011 mit fast 300 Milliarden Euro mehr als 11 Prozent des Bruttoinlandproduktes. Fast 70 Prozent der Kosten im Bereich der „klassischen" Gesundheitsversorgung werden durch die sozialen Sicherungssysteme, überwiegend durch die Gesetzliche Krankenversicherung (GKV) geprägt. Eine weitere Kostensteigerung soll vermieden werden.

Gleichzeitig soll die Versorgungsqualität durch Berücksichtigung von Vorerkrankungen, Wechselwirkungen bei Medikamenteneinsatz und Medizintechnik verbessert werden. Letzteres erfordert eine Kommunikation zwischen den Leistungserbringern und die Integration der Medizintechnik. Für die Prozessintegration sind abrechnungsrelevante und medizinische Daten sektoren- und systemübergreifend bereitzustellen.

Ärzte kommunizieren verstärkt direkt mit den Kassen

Die „Integrierte Versorgung" mit stärkerer Vernetzung verschiedener Fachdisziplinen und Sektoren (Hausärzte, Fachärzte, Krankenhäuser) soll eine nachhaltige Versorgung der Versicherten für bestimmte Erkrankungsfälle ermöglichen. Die Leistungserbringer schließen hierzu „Selektivverträge" mit den Kassen und rechnen diese direkt ab. Hierbei werden neben Abrechnungsdaten oft auch umfangreiche Datensätze mit Patientendaten inklusive kodierter Diagnosen oder Verdachtsdiagnosen, Therapien und Abrechnungsdaten auf elektronischem Wege ausgetauscht.

Will der Arzt neben der direkten Abrechnung mit der GKV weitere Vorteile aus automatisierten Prozessen und Datenaustausch erzielen, muss er mehr Aufwand und Eigenverantwortung für Informationssicherheit und Datenschutz auf sich nehmen – dafür wird er weder bezahlt, noch ist er in der Regel dafür qualifiziert.

Unterstützung können die Kassenärztlichen Vereinigungen (KV) bieten, ein Beispiel ist die Initiative der KV Rheinland-Pfalz, die konkrete Informationen, Handlungshilfen, Checklisten und weiterführende Links zur Gewährleistung von IT-Sicherheit und Datenschutz im Zusammenhang mit einem Praxisbetrieb anbietet.

Integration und Datenkommunikation auch im stationären Bereich

Auch in der stationären Versorgung führen steigende Belastungen und Kostendruck zur Flexibilisierung von Arbeitsprozessen, unter anderen durch verstärkte Vernetzung von Systemen oder dem Fernzugriff auf medizinische Daten.

Für Ärzte in Bereitschaft oder für Spezialisten, die an verschiedenen Kliniken oder an weit verzweigten Campus-Standorten eingesetzt werden, kann der schnelle und direkte Zugriff auf medizinische Daten dem

Über die Telematik-Infrastruktur findet eine Vernetzung aller beteiligten Stellen im Gesundheitswesen statt.

Patienten nützen und gleichzeitig Kosten sparen. Doch selbst ein Fernzugriff auf OP-Belegungspläne oder Reservierungen einer Klink kann für einen Hacker ein interessantes Angriffsziel sein.

Universitätskliniken mit Bereichen für „Forschung und Lehre" müssen das klinische Netz mit medizinischen Daten der dort versorgten Patienten und das Verwaltungsnetz getrennt betreiben. Klinikbetriebe verfügen in der Regel zwar über eigenes IT-Personal, nicht aber immer über eine professionelle IT-Organisation. So bestimmen oft die Ärzte, was an IT-Ausstattung beschafft und wie diese genutzt wird.

Geschäftsleitungen von Kliniken sind über die Stellvertreterhaftung (vgl. § 14 StGB) persönlich verantwortlich und haftbar für das Risiko- und Notfallmanagement (bei privater Rechtsform auch nach dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, KonTraG). Große Universitätskliniken haben bereits ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut und sich nach ISO/IEC 27001 zertifizieren lassen. Vergleichbare Regularien sollten auch für kleinere stationäre Einrichtungen Pflicht werden.

Hochmoderne Medizintechnik als intelligente Netzknoten

Zunehmende Vernetzung und elektronischer Datenaustausch finden sich auch bei medizinischen Geräten zur Diagnose und Therapie. Waren diese früher überwiegend isolierte Geräte mit eventuell einer seriellen Schnittstelle, verfügen sie heute über Netzwerk-Schnittstellen. Medizinische Geräte haben relativ lange Vorlaufzeiten in der Entwicklung, langwierige Zulassungsverfahren und längere Nutzungs-/ Abschreibungszeiten. Da kann das Problem entstehen, dass diese im Kern auf veralteten Betriebssystemversionen basieren (NT4, W2K und bedingt XP), für die es keine Sicherheitsupdates mehr gibt. Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) weist Software als häufigste Fehlerursache in der Kategorie „Design- und Konstruktionsfehler" bei Risikomeldungen aus.

Die Norm DIN EN 62304 definiert zu beachtende Anforderungen an den Lebenszyklus von Software für Medizinprodukte. Zusätzlich sollte das Thema Informationssicherheit fest in den Entwicklungsprozess verankert und dieser als „Secure Development Lifecycle" (SDL) abgebildet werden.

eGK und Telematik-Infrastruktur

Die Einführung der elektronischen Gesundheitskarte (eGK), des Heilberufeausweises (HBA) sowie der Telematik-Infrastruktur (TI) der gematik ist eines der größten IT-Projekte in Deutschland. Ziel ist die lebenslange Speicherung wesentlicher Behandlungsdaten möglichst aller Versicherten auf zentralen Servern bei hohen Ansprüchen an Datenschutz und Informationssicherheit.

Zum aktuell laufenden Rollout der Stufe 1 gehören zunächst nur die Telematik-Infrastruktur (Basis-TI) sowie das Versichertenstammdatenmanagement (VSDM). Später soll zusätzlich die Qualifizierte elektronische Signatur (QES), zum Beispiel für Ärztebriefe, erprobt werden. Weitere Anwendungsfälle der eGK wie Rezepte, Notfalldaten, Blutgruppe, Verwahrungsort einer Patientenverfügung oder Organspenderstatus werden frühestens 2018 projektiert.

Angesichts der Sorge um mangelnde Datensicherheit und jüngster Abhörpraktiken der Geheimdienste steht dieses Projekt umso mehr in heftiger Kritik. Tatsächlich fehlt formal noch der Nachweis der Tauglichkeit nach ISO/IEC 15408 gegenüber dem BSI.

ePA vs. EFA

In der TI sollen vollständige Patientendaten dauerhaft als elektronische Patientenakte (ePA) gespeichert werden. Die elektronische Fallakte (EFA) ist eine Plattform nur für Ärzte zum datenschutzgerechten Austausch medizinischer Daten von gemeinsam behandelten Patienten über Sektor- und Einrichtungsgrenzen hinweg. Sie wird für einen medizinischen Fall angelegt und hat eine definierte „Lebensdauer". Die Daten liegen dezentral bei der jeweils verantwortlichen Einrichtung beziehungsweise beim behandelnden Arzt. Ein sogenannter EFA-Provider mit ausreichend professionellem IT-Betrieb und Erfüllung rechtlicher Rahmenbedingungen speichert die Dokumentenstruktur und Quellenangaben der zugehörigen Dokumente beziehungsweise Kopien davon.

EFA arbeitet webbasiert, ist seit Version EFA2.0 IHE-konform (IHE, Integrating the Healthcare Enterprise) und unterstützt somit auch internationale Kommunikationsstandards wie DICOM (Radiologie) und HL7 (Krankenhäuser). Später werden die EFA-Daten als funktionaler Gesundheitsdatendienst (GDD) in die Telematik-Infrastruktur migriert.

DriveLock
Daten intelligent schützen

Ihre Sicherheitslösung wartet bereits auf Sie!
Schützen Sie sich jetzt – mit DriveLock.

DriveLock ist die Antwort.

VERSCHLÜSSELUNG.
Durch die zertifizierte Verschlüsselung von DriveLock vermeiden Sie Datendiebstahl und -verluste. Egal ob auf Datenträgern oder bei Daten in der Cloud.

ANTIVIRUS.
DriveLock Antivirus bietet optimalen Schutz vor externen Bedrohungen bei maximaler Flexibilität, mit einfacher und intuitiver Bedienung.

SICHERHEITSBEWUSSTSEIN.
DriveLock unterstützt Sie aktiv mithilfe von zeitlich gesteuerten Sicherheitskampagnen und steigert das Sicherheitsdenken der Mitarbeiter.

SCHNITTSTELLENKONTROLLE.
Der zentral konfigurierbare Zugriff von DriveLock ermöglicht eine fein abgestimmte Kontrolle über sämtliche Laufwerkstypen und Rechtemodelle.

APPLIKATIONSKONTROLLE.
Bei minimalem Konfigurationsaufwand legen Sie fest, welche Anwendungen von wem auf welchem Gerät genutzt werden – und welche nicht.

Testversion JETZT downloaden!
› WWW.DRIVELOCK.DE

CenterTools

Fazit

Nur mit Technik kann man die Anforderungen an Datenschutz und Informationssicherheit nicht erfüllen, die fortschreitende Integration und Automatisierung ist auch nicht zu verhindern. Regulierung, Kontrolle, Awareness und Vertrauensbildung bei allen Beteiligten müssen die Eckpfeiler eines zu fordernden Sicherheitsniveaus sein und mit konkreten Maßnahmen begleitet werden:

— Analyse und Dokumentation der Prozesse bei den Leistungserbringern
— ggf. Einführung von ISMS-Lösungen
— Identifikation und Bewertung von Risiken
— Definition geeigneter (Notfall-) Maßnahmen
— Regelmäßige Sicherheitsüberprüfung von Netzgrenzen, Systemen und Softwarelösungen
— Reviews bestehender Softwarelösungen auch unter Sicherheitsaspekten
— Sicherheit im Entwicklungsprozess verankern (SDL)

Unkontrollierter Datenaustausch im Gesundheitswesen muss verhindert werden; dagegen stellt eine bundesweite, regulierte und sichere Telematik-Infrastruktur für sensible Gesundheitsdaten tatsächlich eine wünschenswerte Lösung dar. Mit der eGK als Schlüssel und der freiwilligen Teilnahme wird auch das Recht des Bürgers auf informationelle Selbstbestimmung sichergestellt.

Elektronische Gesundheitskarte (eGK)

Aufschwung für ISO 27001 und BSI IT-Grundschutz

Die Einführung der elektronischen Gesundheitskarte (eGK) hat nicht nur Auswirkungen auf die IT im Gesundheitswesen, sondern auf das Informationssicherheits-Managementsystem der beteiligten Institutionen insgesamt.

Von Randolf-Heiko Skerka, SRC Security Research & Consulting GmbH

Nicht zuletzt die Schlagzeilen zum Diebstahl der Krankenakte von Michael Schumacher haben deutlich gemacht, dass insbesondere im Gesundheitswesen die Informationssicherheit einen sehr hohen Stellenwert genießt. Es wird in diesem öffentlichkeitswirksamen Fall davon ausgegangen, dass die sensiblen Inhalte durch einen Angriff auf die Computersysteme des Universitätsklinikums abhanden gekommen sind. Ob dies tatsächlich so war, muss durch entsprechende forensische Untersuchungen geprüft werden. Hinsichtlich des Schutzes von Gesundheitsdaten darf allerdings der Blick nicht nur auf der Informationstechnik (IT) ruhen, sondern es müssen Informationen in allen Bereichen einer Organisation geschützt werden – daher spricht man auch von „Informations"- und nicht nur von „IT"-Sicherheit.

Ein Informationssicherheits-Managementsystem (ISMS) ist ein ganzheitlicher Ansatz, sensible Informationen einer Organisation jederzeit angemessen zu schützen und Schäden durch Manipulation oder Verlust der Informationen auf ein akzeptables Maß zu begrenzen. Die bekanntesten Normen für ISMS sind die ISO/IEC 27001, ISO/IEC 27002 und ihre ergänzenden Standards (ISO/IEC 2700x), sowie die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Normenfamilie ISO/IEC 2700x stellt speziell für den Gesundheitssektor die ISO/IEC 27799 bereit, die auf dessen spezifische Belange eingeht.

Man sollte meinen, dass die Etablierung eines Managementsystems zum Schutz von Informationen im Interesse aller Organisationen sein sollte. Die Realität sieht jedoch oft anders aus. ISMS werden in der Regel erst dann etabliert, wenn externe Anforderungen dies erforderlich machen. Im deutschen Gesundheitswesen erfolgt die Umsetzung von ISMS mit der Einführung der elektronischen Gesundheitskarte.

Relevanz eines ISMS im Gesundheitswesen

Die im Mai 2014 veröffentlichte Studie „European Hospital Survey - Benchmarking Deployment of eHealth Services (2012-2013)" macht deutlich, dass im Gesundheitssektor noch viel Platz für Verbesserungen

ist. Exemplarisch wird dies durch den Umstand deutlich, dass nur in 37 Prozent der Fälle Daten verschlüsselt gespeichert werden. Bei vielen Außenstehenden dürfte dies für Verwunderung sorgen. Auch in Deutschland (40 %) ist die Situation nicht besser, schaut man sich im Vergleich hierzu Großbritannien (80 %), Finnland (69 %) oder Luxemburg (67 %) an.

Für Organisationen, die im Gesundheitssektor tätig sind und hier insbesondere für den schweigepflichtigen Personenkreis gemäß § 203 StGB, dürfte das Thema ISMS zukünftig an Bedeutung gewinnen, insbesondere, da noch immer Patientenakten im Altpapier landen [1].

Zwar lässt sich durchaus wahrnehmen, dass IT-Dienstleister, die im Gesundheitssektor tätig sind, Informationssicherheits-Managementsysteme etablieren und zertifizieren, bei den Leistungserbringern scheinen solche Themen jedoch eine noch untergeordnete Priorität zu haben, obwohl die genannten speziellen Standards bereits existieren.

Das Thema ISMS im Gesundheitssektor wird durch die Einführung der elektronischen Gesundheitskarte (eGK) an Relevanz gewinnen. Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) hat Anforderungen an die Telematikinfrastruktur (TI) und ihre Bestandteile in verschiedenen Konzepten und Spezifikationen festgelegt [2]. In diesen werden auch die Sicherheitsanforderungen für Betreiber und Anbieter von Dienstleistungen in der TI definiert. Hiermit soll sichergestellt werden, dass zum Beispiel die Anforderungen an die Sicherheit der Plattform für die Anwendungen der elektronischen Gesundheitskarte gewährleistet sind. Denn nur wer die Vorgaben der gematik vollständig umsetzt, darf an der TI teilnehmen.

Anforderungs-ID der gematik	Anforderung
GS-A_4980	**Umsetzung der Norm ISO/IEC 27001** Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN für genau die Umgebungen, in denen diese Produkte betrieben werden, die internationale Norm ISO/IEC 27001 umsetzen.
GS-A_4981	**Erreichen der Ziele der Norm ISO/IEC 27001 Annex A** Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN für genau die Umgebungen, in denen diese Produkte betrieben werden, zu allen gemäß der Erklärung der Anwendbarkeit (engl. „Statement of Applicability") anwendbaren Maßnahmen (engl. „controls") der internationalen Norm ISO/IEC 27001 ergreifen und die dort angegebenen Ziele (engl. „objectives") erreichen.
GS-A_4982	**Umsetzung der Maßnahmen der Norm ISO/IEC 27002** Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten SOLLEN für genau die Umgebungen, in denen diese Produkte betrieben werden, bei Ergreifung der Maßnahmen (engl. „controls") aus der internationalen Norm ISO/IEC 27002 die dort angegebene „Anleitung zur Umsetzung" (engl. „implementation guidance") und die dort angegebenen „Weiteren Informationen" (engl. „other information") befolgen.
GS-A_4983	**Umsetzung der Maßnahmen aus dem BSI-Grundschutz** Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fach-anwendungsspezifischen Diensten SOLLEN für genau die Umgebungen, in denen diese Produkte betrieben werden, bei der Umsetzung der internationalen Normen ISO/IEC 27001 und ISO/IEC 27002 die zugehörigen Maßnahmen des BSI-Grundschutzkatalogs umsetzen (vgl. Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz des BSI).
GS-A_3784	**Nachweis durch ISO27001 Zertifikat** Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fach-anwendungsspezifischen Diensten KÖNNEN zum Nachweis der Umsetzung der Anforderungen an die Betriebsumgebung ihre Dienste und das ISM der Beteiligten eine ISO 27001-Zertifizierung mit einem Geltungsbereich, der den betriebenen Dienst und die unterstützenden Systeme umfasst, durchführen.
Kap. 3.3 gemRL_ PruefSichEig_DS	**Einhaltung der Vorschriften zum Schutz der personenbezogenen Daten** Die Grundschutzmaßnahmen des ergänzenden Maßnahmenbündels für den Bereich Datenschutz (BSI Baustein B1.5) MÜSSEN für alle IT-Systeme und IT-Verfahren, die personenbezogene Daten verarbeiten, geprüft werden und in der Domäne Datenschutz dargestellt werden.

Anforderungen an Betreiber und Anbieter

In der Projektphase „Basis-Rollout – Erprobung und Produktivbetrieb“ sind die Anforderungen der gematik in verschiedenen Dokumenten niedergelegt. Einen Überblick bildet die „Dokumentenlandkarte Online-Rollout (Stufe 1) - Erprobung und Produktivbetrieb“ [3], welche insbesondere einen Überblick über die verbindlichen Konzepte und Spezifikationen der gematik beinhaltet.

Die gematik bezeichnet zulassungspflichtige Objekte als „Komponenten und Dienste“, Anforderungen an die Komponenten und Dienste werden in den Produkttypsteckbriefen zusammengefasst. Diese können wiederum auf Konzepte und Spezifikationen verweisen, deren Anforderungen mit umzusetzen sind. Die gesammelten Anforderungen können sehr unterschiedliche Niveaus aufweisen – von Forderungen an TLS-Verbindungen bis zur Zertifizierung eines ISMS.

Produkttypsteckbriefe existieren für diverse dezentrale Komponenten, PKI-Produkttypen, zentrale Dienste und Fachanwendungen der TI, wie dem Fachdienst für das Versichertenstammdatenmanagement (VSDM). Über ein VSDM kann der Versicherte zum Beispiel online die Aktualität der auf der Karte gespeicherten Versichertenstammdaten überprüfen und bei Bedarf aktualisieren, ohne dass die Karte ausgetauscht werden muss.

Jeder Anforderung in den Produkttypsteckbriefen ist eine Anforderungs-ID (Afo-ID) zugeordnet, die durch den Betreiber umzusetzen und im Rahmen eines Sicherheitsgutachtens durch zugelassene Gutachten zu prüfen ist. Für den Fachdienst VSDM sind dies beispielsweise 60 Anforderungen, die durch einen Betreiber umzusetzen und einen Gutachter zu bestätigen sind.

ISO/IEC 27001 und IT-Grundschutz-Kataloge

Die Produkttypsteckbriefe, Konzepte und Spezifikationen beinhalten neben technischen Anforderungen auch solche, die an Prozesse oder Organisationen gestellt werden. Zusätzlich zu den jeweiligen Produkttypsteckbriefen und Spezifikationen sind für die Betreiber insbesondere die gematik-Dokumente „Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI“ und „Richtlinie zur Prüfung der Sicherheitseignung“ von Bedeutung.

Betrachtet man die Summe der für einen Betreiber relevanten Anforderungen, stellt man schnell fest, dass die gematik an vielen Stellen Aspekte der ISO/IEC 27001, ISO/IEC 27002 und der IT-Grundschutz-Kataloge aufgegriffen hat. Explizit wird in verschiedenen Produkttypsteckbriefen auf die folgenden Anforderungen der „Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI“ und der „Richtlinie zur Prüfung der Sicherheitseignung“ verwiesen (vgl. Tabelle 1).

Gerade die Anforderungen GS-A_4980 (Umsetzung der Norm ISO/IEC 27001) und GS-A_4983 (Umsetzung der Maßnahmen aus dem BSI-Grundschutz) stellen einen direkten Bezug zur ISO/IEC 27001 und den IT-Grundschutz-Katalogen dar.

Was bedeutet dies für ISO 27001?

Im Rahmen eines für die Zulassung durch die gematik zu erstellenden Sicherheitsgutachtens wird sich herausstellen, dass die Aufwände für die Prüfung der Anforderungen GS-A_4980 und GS-A_4983 den Umfang eines vollständigen ISO/IEC 27001 Audits annehmen werden. Obwohl eine formale Zertifizierung nach diesem Standard für die gematik Zulassung nicht erforderlich ist, wird ein Betreiber der jeweiligen Komponenten und Dienste schnell feststellen, dass es im Zulassungsverfahren der gematik von Vorteil sein wird, die als „optional“ gekennzeichnete Anforderung GS-A_3784 (Nachweis durch ISO27001 Zertifikat) zu erfüllen, um dann den Zulassungsprozess zu optimieren und einen Mehrwert zu erhalten.

Da die gematik-Zulassung zeitlich befristet ist, wird sich spätestens bei der Wiederholungsbegutachtung nach drei Jahren zeigen, dass der Aufwand für die Fortführung der gematik-Zulassung bei einem ISO 27001-zertifizierten ISMS geringer ist als im anderen Fall. Zu ähnlichen Entwicklungen kam es in der Vergangenheit bei anderen regulierten Branchen (Energiesektor, Glückspielbranche). Es ist also zu erwarten, dass sich in den nächsten Jahren die Betreiber von Systemen in der TI zunehmend einer Zertifizierung nach ISO/IEC 27001 unterziehen werden, da das Zulassungsverfahren der gematik ohnehin die Prüfung auf Konformität zur ISO/IEC 27001 fordert. ■

Literatur

[1] www.focus.de/regional/hessen/datenschutz-nicht-gesicherte-patientenakten-gefunden_id_3823810.html
[2] www.gematik.de/cms/de/spezifikation/spezifikation_startseite.jsp
[3] www.gematik.de/cms/media/dokumente/ors1_release_1_2/gematik_Dokumentenlandkarte_Rel_1_2_0~1.pdf

KV-S@feNet
zertifizierter Provider

TELEMED @
Kommunikationslösungen

Sicher online im Gesundheitswesen.

Praxissysteme schützen, Patientendaten sichern.

- **KV-SafeNet Marktführer – bundesweit!**
- **Sicherer und datenschutzkonformer Online-Zugang**
- **Mobile Heimarbeit weltweit – auch mit Tablets**
- **Virenschutz für Praxis-PC`s**

CompuGroup Medical Deutschland
Geschäftsbereich telemed
Maria Trost 21, 56070 Koblenz
T +49 (0) 261 8000-2007
F +49 (0) 261 8000-2029
info@telemed.de

telemed.de
cgm.com/de

Synchronizing Healthcare

CGM CompuGroup Medical

Leben mit dem Risiko oder Lebensrisiko?

IT-Sicherheits- und Risikomanagement in Krankenhäusern unterentwickelt

IT ist eine der wichtigsten Ressourcen im heutigen Krankenhausbetrieb. Die zunehmende IT-Durchdringung hat zur Folge, dass Krankenhäuser vermehrt von IT-Ausfällen, Schadsoftware und anderen Sicherheitsvorfällen betroffen sind. Der Bedarf, die eigene IT zu schützen, ist durchaus erkannt. Konkretes Handeln scheitert kläglich an der gelebten Wirklichkeit im Krankenhaus.

Von Rolf Irion und Dr. Werner A. Knetsch, HiScout GmbH

Das Risikoportfolio von Krankenhäusern beziehungsweise Klinikbetreibern sucht inzwischen seinesgleichen. Neben den medizinischen Behandlungs- und Hygienerisiken finden sich im Jahre 2014 auch vermehrt betriebliche Risiken, die aus dem verstärkten Einsatz von Medizintechnik, medizinischer und allgemeiner Informations- und Kommunikationstechnologie (IKT) resultieren.

Das hat auch der Gesetzgeber erkannt. Die Verpflichtung der Krankenhäuser, ein übergreifendes Risikomanagement einzuführen, ergibt sich zum Beispiel aus dem Sozialgesetzbuch (§ 137 Absatz 1d SGB V). Andernfalls ist die Kassenzulassung gefährdet. Auch der bereits 1998 verschärfte § 91 II des Aktiengesetzes (AktG) verpflichtet zur Einführung. Dies gilt insbesondere für Betreibergesellschaften und Kliniken in der Rechtsform einer AG; die Pflicht strahlt aber auch auf andere Rechtsformen wie die GmbH aus.

Unabhängig von der Rechtsform und Größe stellt zusätzlich der Schutz von Patientendaten vor Verlust, Diebstahl und Manipulation eine besondere Verpflichtung und Herausforderung für Krankenhausbetreiber und medizinisches Personal dar. Verschärft werden diese Anforderungen durch das absehbare IT-Sicherheitsgesetz, welches Krankenhäuser als kritische Infrastruktur klassifiziert.

Der zunehmende Einsatz moderner IKT und deren Vernetzung mit medizinischen Geräten zu komplexen medizinischen IT-Netzwerken führen zu einer neuen Qualität und erhöhten Komplexität der inhärenten Risiken mit großem Schadenspotenzial für die Patienten. Diesem Risiko wird bisher kaum begegnet, obwohl IKT im IT-Betrieb Krankenhaus ein Leistungsfaktor ist, der moderne klinische Prozesse von Anamnese, Diagnose bis zur Therapie überhaupt erst ermöglicht.

Die Wirklichkeit

Die im Jahr 2011 veröffentlichte DIN EN 80001-1 regelt das Risikomanagement für IT-Netzwerke, die Medizinprodukte enthalten, mit klaren Vorgaben. Noch hat diese Norm keinen Gesetzescharakter. Gleiches gilt für den Leitfaden des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Risikoanalyse Krankenhaus-IT (www.kritis.bund.de). Doch schon jetzt dokumentiert sie den aktuellen Stand der Technik. Für den Fall der Nichtbeachtung ihrer konkreten Vorgaben und Anforderungen im Kontext nachgewiesener Versäumnisse für die verantwortlich handelnden Personen wie zum Beispiel Klinikleiter und leitende Ärzte kann sie daher im Schadensfall ein erhebliches persönliches Haftungsrisiko begründen.

Die Betroffenen beziehungsweise Verantwortlichen scheinen aber den Kopf in den Sand zu stecken. So jedenfalls unser Eindruck aus vielen Gesprächen und Diskussionen mit Vertretern von Häusern der Zentral- und Regionalversorgung zu dieser Thematik. Nach unserer Erkenntnis herrscht eine eklatante Diskrepanz zwischen dem formellen Anspruch und der gelebten Praxis. Informationssicherheits- und Risikomanagement in deutschen Kliniken wird nicht die Bedeutung beigemessen, die ihnen zukommt. Dort wo Initiativen betrieben werden, stecken diese häufig in den Anfängen, mancherorts haben sie rein prätentiösen Charakter.

Die meisten deutschen Krankenhäuser sind daher heute bezüglich der formellen Anforderungen an IT-Sicherheit, Datenschutz und Risikomanagement „non-compliant“. Ein Tatbestand, der im Rahmen von Betriebs- und Wirtschaftsprüfungen oder juristischen Auseinandersetzungen Relevanz erhalten wird.

Die Hürde

In der klinischen Praxis sehen wir, dass der Reifegrad von IT-Managementprozessen durchweg unterentwickelt, wenn überhaupt

existent ist (siehe Abbildung 1). Im Vergleich zu Branchen, wie zum Beispiel Banken und Versicherungen, hinkt das IT-Management im Krankenhaus um Jahre hinterher, obwohl beide zu den sogenannten kritischen Infrastrukturen zählen.

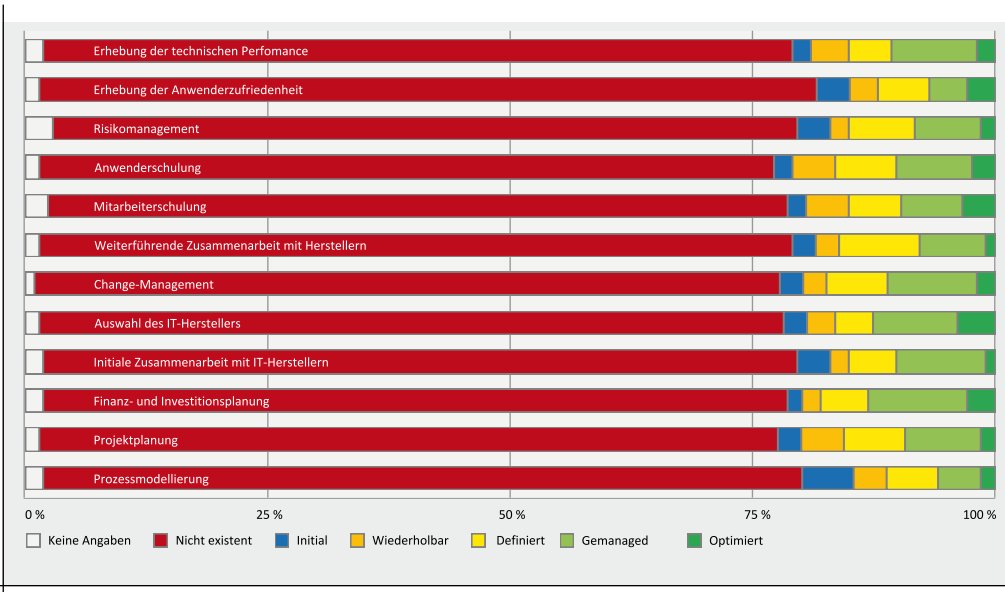
Eine von HiScout durchgeführte Marktexploration stellte fest, dass bei vielen IT- und Risikoverantwortlichen das Bewusstsein für Risiken und Sicherheitsfragen vorhanden ist und sie die offensichtlichen Defizite durchaus erkennen. Die von ihnen vorgetragenen Initiativen scheitern dann regelmäßig an fehlender Unterstützung im Krankenhaus-Management und/oder Budgetlimitationen als Ausdruck einer reinen Kostenbetrachtung der Krankenhaus-IT [1].

Das Problem kann folgendermaßen beschrieben werden: „Die Krankenhäuser investieren nicht in die IT. Weshalb auch, die kostet ja nur. […] Wer aber nicht investiert (in Material und v. a. Menschen), für den gilt der Spruch ‚you get what you pay for'." [2] Das erklärt auch den niedrigen Reifegrad von Krankenhäusern und Klinikbetreibern im IT-Service Management. Die Krankenhaus-IT wird so zum schwächsten Glied der Kette.

Der Handlungswille

Die Krankenhaus-IT ist dafür verantwortlich, die negativen Konsequenzen der reinen Kostenbetrachtung für das IT-Management aufzuzeigen. Dazu sind die erkannten Defizite gegenüber der Leitung offensiv zu vertreten, transparent zu machen und mögliche Konsequenzen des Nicht-Handelns zu verdeutlichen.

In einem ersten Schritt wird durch die Einführung eines IT-Service-Managements mit einem nennenswerten Reifegrad der Flaschenhals für ein IT-Sicherheits- und Risikomanagement, das auch IT-Netzwerke mit Medizinprodukten umfasst, beseitigt. Im nächsten Schritt oder begleitend muss mit der Einführung eines „Information Security Management Systems" (ISMS) nach BSI-Grundschutz oder ISO/IEC 27001-27799 „IT-Sicherheit im Gesundheitswesen" begonnen werden.



Reifegrad der IT-Management-Prozesse (n=206), Quelle: IT-Report Gesundheitswesen, Schwerpunkt IT-Unterstützung klinischer Prozesse, S. 79

Erst dann bietet es sich an, im Rahmen eines überschaubaren und ressourcenschonenden Pilotprojekts zum Risikomanagement in medizinischen IT-Netzwerken erste Erfahrungen zu sammeln, eine standardisierte Vorgehensweise zu entwickeln sowie einen Risikomanagement-Prozess zu etablieren und nachfolgenden Projekten als erprobtes Vorgehensmodell zur Verfügung zu stellen. Iterativ sollte dann ein medizinisches IT-Netzwerk nach dem anderen betrachtet werden. Die Erfahrungen fließen jeweils wieder in Vorgehensweise, Prozesse und Organisation ein.

Der Einsatz eines geeigneten ISMS-Tools mit einer integrierten Risikoanalyse ermöglicht es, diesen Prozess effizient zu etablieren und entsprechend der Lernkurve des Kunden weiter auszubauen. Informationssicherheits- und Risikomanagement im Gesundheitswesen ist ein ganzheitlicher Prozess, der sowohl die Klinikverwaltung als auch die IT, Medizin-IT, Medizintechnik, das Pflegepersonal und auch die Ärzteschaft umfasst. Alle genannten Personengruppen sind hier gleichermaßen angesprochen.

Ausgangspunkt für eine Initiative hinsichtlich IT-Service Management und IT-Sicherheit kann eine Reifegradermittlung der IT sein. Diese wird später hinsichtlich ISMS allgemein und ITSM regelmäßig überprüft, der Fortschritt dokumentiert und ein Fahrplan erarbeitet, wie der aktuelle Stand der Technik umgesetzt und der Reifegrad kontinuierlich erhöht werden können.

Anschließend wächst das IT- und Risiko-Managementsystem mit. Die Wissensbasis wird größer, Lerneffekte kommen hinzu, der Reifegrad in den involvierten Teilbereichen steigt und nach und nach werden weitere Standorte oder Kliniken aufgeschaltet.

Literatur

[1] www.aerzteblatt.de/archiv/65744/IT-Sicherheit-im-Gesundheitswesen-Budgets-unzureichend Stand: 30.06.2014.
[2] www.johner-institut.de/wissen/2014/gesundheitswesen/krankenhaeuser-it-maessig-auf-dem-stand-der-2000er#more-7740 Stand: 28.06.2014.

Überarbeitete „Orientierungshilfe Krankenhausinformationssysteme“

Langer Weg braucht langen Atem

Die datenschutzkonforme Gestaltung der Krankenhaus-IT steht bereits seit einigen Jahren auf der Agenda der Datenschutzbeauftragten des Bundes und der Länder. Die überarbeitete und im März 2014 veröffentlichte „Orientierungshilfe Krankenhausinformationssysteme“ stellt die dabei maßgebenden rechtlichen und technischen Gesichtspunkte dar. Der Beitrag beschreibt Hintergrund, Entwicklung und Sachstand des Papiers und seine Auswirkungen.

Von Helmut Eiermann, Leiter des Bereichs Technik beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Mainz

Wie in anderen Lebensbereichen auch, hat der Einsatz der Informationstechnik Abläufe und Geschäftsprozesse im Krankenhaus grundlegend verändert. Krankenhausinformationssysteme (KIS) sind zu unverzichtbaren Hilfsmitteln der Krankenhausbehandlung geworden. Ihre Daten bilden die Grundlage effizienter Behandlungsprozesse und -entscheidungen.

Die Digitalisierung im Gesundheitswesen hält neben den sich ergebenden Chancen für eine effizientere Gesundheitsversorgung naturgemäß auch Datenschutzrisiken bereit. Die Möglichkeiten, Behandlungsdaten einzusehen, sind vielfältig, weitreichend und nicht immer durch begleitende Sicherungsmaßnahmen eingehegt. Eine Reihe bekanntgewordener Fälle zeigt, dass Behandlungsdaten von Bekannten, Familienangehörigen, Arbeitskollegen oder Personen des öffentlichen Lebens nicht nur fachliches Interesse wecken und wiederholt missbräuchlich verwendet wurden.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf Patientendaten grundsätzlich nur denjenigen möglich sein darf, die an der Behandlung medizinisch, pflegerisch oder zur verwaltungsmäßigen Abwicklung beteiligt sind. Die Funktionalität der eingesetzten IT-Lösungen und deren Konfiguration, Betrieb und Nutzung in den Krankenhäusern müssen dem entsprechen. Die Krankenhäuser stehen in der Pflicht, ihre KIS-Systeme datenschutzgerecht zu betreiben und die Hersteller sind gehalten, entsprechende Lösungen anzubieten.

Die Notwendigkeit, beide Seiten - Betreiber und Hersteller - in den Blick zu nehmen, ergab sich aufgrund der Tatsache, dass Prüfungen der Datenschutzbeauftragten häufig eine „Deadlock“-Situation aufzeigten: Defizite wurden seitens der Krankenhäuser meist mit fehlenden Funktionen der jeweiligen KIS-Lösung begründet und seitens der Hersteller damit, dass von den Kunden keine entsprechenden Anforderungen gestellt wurden. Ein Großteil der am Markt angebotenen Lösungen blieb nach den Erkenntnissen der Datenschutzbeauftragten damit hinter den datenschutzrechtlichen Anforderungen zurück.

Je nach Standort und Trägerschaft der Einrichtungen gelten dabei unterschiedliche Rechtsvorgaben (Landeskrankenhausgesetze, Bundesdatenschutzgesetz, kirchliche Datenschutzordnungen). Um zu einem trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, wurde unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche im März 2011 die „Orientierungshilfe Krankenhausinformationssysteme“ erarbeitet. Diese sollte es Betreibern und Herstellern von Krankenhausinformationssystemen erleichtern, den gesetzlichen Anforderungen gerecht zu werden.

Anhand musterhafter Vorgaben beschreibt die Orientierungshilfe Maßnahmen bei der Gestaltung und dem Betrieb von KIS-Lösungen. Diese betreffen das Datenmodell eines Krankenhausinformationssystems, notwendige System- und Anwendungsfunktionen, die Rollen- und Berechtigungskonzeption, den Umfang einer notwendigen Protokollierung und deren Auswertung sowie den technischen Betrieb und die Administration.

Den Empfehlungen liegt ein typisiertes Krankenhausmodell zugrunde, um angesichts der vorliegenden Bandbreite der Häuser - vom kleinen selbstständigen Kreiskrankenhaus über die Zwittergestalt der Universitätskliniken bis zum Krankenhauskonzern mit einer Vielzahl von Einrichtungen - eine funktionale Basis für die Empfehlungen zu legen. Die Empfehlungen sind daher exemplarisch und lassen Raum für Alternativen, die das gleiche Schutzniveau oder die gleiche Funktionalität gewährleisten.

Dieser Ansatz war nicht unumstritten und wurde insbesondere seitens der Krankenhausverbände problematisiert. Die Diskussion im Rahmen exemplarischer Umsetzungsprojekte und Prüfungen zeigt

jedoch, dass dieses Modell weiterhin trägt. Obschon die Entwicklung in den Krankenhäusern in vielen Fällen zu einer Auflösung bisheriger Strukturen geführt hat, verfügt der Großteil nach wie vor über eine klassische Organisationsstruktur mit Fachabteilungen bzw. ist dieses Konzept in vielen KIS-Lösungen abgebildet.

Entwicklung - Was hat sich getan?

Mit der Orientierungshilfe Krankenhausinformationssysteme wurde das Thema „Datenschutz im Krankenhaus" in die öffentliche Diskussion gerückt. Dabei kam es zu durchaus unterschiedlichen Bewertungen. Einigkeit bestand jedoch immer über die Notwendigkeit der datenschutzgerechten Ausgestaltung der im Krankenhaus genutzten Informationstechnik. Ergänzt wurde der Austausch mit Herstellern und Betreibern, der Deutschen Krankenhausgesellschaft und Landeskrankenhausgesellschaften durch Pilotprojekte zur Umsetzung der Anforderungen der OH KIS, Sachstanderhebungen und nicht zuletzt durch entsprechende Prüfungen der Datenschutzaufsichtsbehörden.

Die Erkenntnisse flossen in die überarbeitete Fassung der Orientierungshilfe vom März 2014 ein. Ergänzend hierzu hat die Deutsche Krankenhausgesellschaft ein Grundsatzpapier mit Hinweisen und Musterkonzepten für die Umsetzung der technischen Anforderungen erstellt.

Der Dialog mit Herstellern, Betreibern und Verbänden hat zu spürbaren Verbesserungen geführt. Viele Hersteller legen die Orientierungshilfe mittlerweile ihrer Produkt- und Entwicklungsplanung zugrunde und Krankenhäuser übernehmen die Anforderungen in Ausschreibungen zur Beschaffung von KIS-Lösungen. Trotz nach wie vor bestehender Defizite ist damit die Grundlage für eine nachhaltige Verankerung der Datenschutzaspekte in KIS-Lösungen gelegt.

Wie ist die aktuelle Situation?

Auf der Grundlage der Orientierungshilfe führen die Datenschutzbeauftragten Prüfungen in Krankenhäusern durch, um zu klären, inwieweit die Empfehlungen in den IT-Lösungen und Geschäftsprozessen der Krankenhäuser ihren Niederschlag gefunden haben. In Rheinland-Pfalz erfolgt dies im Rahmen einer Querschnittskontrolle, die Häuser unterschiedlicher Größe und Betreibermodelle erfasst. Die bislang vorliegenden Ergebnisse lassen erkennen, dass nach wie vor Defizite bestehen. Diese liegen sowohl in der Verantwortung der Hersteller als auch der Betreiber und betreffen vor allem folgende Bereiche:

— **Oftmals zu weit gefasste Zugriffsrechte in den KIS-Systemen**
Ursächlich dafür sind einerseits fehlende Konzepte für die Vergabe von Berechtigungen. Häufig sind diese historisch gewachsen und gründen nicht auf konzeptionellen Überlegungen zu fachlichen oder organisatorischen Notwendigkeiten. Andererseits mangelt es an Funktionen in den KIS-Lösungen, die es erlauben, Zugriffe auf die konkret zu behandelnden Patienten zu beschränken bzw. deren Daten fallweise zur Verfügung zu stellen.

— **Fehlende Sperr- und Löschfunktionen**
Trotz entsprechender gesetzlicher Regelungen sind nach Abschluss einer Behandlung notwendige Zugriffsbeschränkungen und Löschungen nicht umgesetzt. Auch wenn für die Speicherung der Daten aus einer Behandlung vergleichsweise lange Speicherfristen zugrunde gelegt werden, entbindet dies die Betreiber nicht von der Differenzierung nach medizinischen, Abrechnungs- und Verwaltungsdaten und einer Prüfung auf deren weitere Notwendigkeit. Für die Aufgabenerfüllung nicht mehr erforderliche Daten sind nach den gesetzlichen Vorgaben zu löschen. Als problematisch erweist sich hierbei, dass nach wie vor eine Reihe von KIS-Lösungen keine wirksame Löschung von Daten ermöglicht und damit in der Konsequenz nicht als datenschutzkonform angesehen werden kann.

— **Mangelnde Nachvollziehbarkeit der Zugriffe auf Patientendaten**
Angesicht der Komplexität von KIS-Lösungen und der Verlässlichkeit und Sensibilität von Behandlungsdaten muss eine nachträgliche Überprüfung von Zugriffen auf ihre Zulässigkeit und ihren Umfang möglich sein. Neben ändernden Zugriffen betrifft dies insbesondere lesende Zugriffe auf Patientendaten (vgl. Urteil des Europäischen Gerichtshofs ECHR Application No. 20511/03). Hier zeigt sich, dass in der Praxis häufig konzeptionelle Überlegungen zur Protokollierung der KIS-Nutzung und der Auswertung und Löschung von Protokolldaten als auch eine valide Protokollierung fehlen.

Die Diskussion um die Orientierungshilfe Krankenhausinformationssysteme hat gezeigt, dass technische Anforderungen, Strukturen und Prozesse im Krankenhausbetrieb einem dynamischen Wandel unterworfen sind und Datenschutzaspekte parallel mitgedacht werden müssen. Es bleibt zu hoffen, dass die mit der Veröffentlichung der Orientierungshilfe erzeugte Dynamik bei der weiteren Entwicklung und dem Einsatz von KIS-Lösungen in der Praxis zu konstruktiven und nachhaltigen Lösungen führt. ■

Literatur

Entschließung der 87. Datenschutzkonferenz zur datenschutzkonformen Gestaltung und Nutzung von Krankenhausinformationssystemen, http://s.rlp.de/ZWF

Orientierungshilfe Krankenhausinformationssysteme (Version 2 vom März 2014), http://s.rlp.de/ohkisv2

Hinweise und Musterkonzepte der deutschen Krankenhausgesellschaft für die Umsetzung der technischen Anforderungen der OH KIS, http://s.rlp.de/m8g

Unterlagen des LfDI Rheinland-Pfalz zur Umsetzung der OH KIS, http://s.rlp.de/AIS

Kein Blutdruck beim Thema Datenschutz hat weitreichende Folgen

Gesundheitseinrichtungen wie Krankenhäuser und Arztpraxen haben mit der Einhaltung des hippokratischen Eids eine verantwortungsvolle Aufgabe. Neben der medizinischen Versorgung von Patienten haben Personen in medizinischen Berufen allerdings weitere verantwortungsvolle Tätigkeiten, die erledigt werden müssen, damit zum Beispiel Datenschutzskandale keine Chance haben.

Von Stefanie Keller, HSM GmbH + Co. KG

Theoretisch müsste die medizinische Branche den Umgang mit sensiblen und personenbezogenen Daten gewohnt sein. Doch die Erfahrungen und die diversen Datenschutzskandale in den Medien zeigen, dass trotzdem allzu oft Dokumente im Papierkorb oder Papiercontainer landen und somit durch unvorsichtiges Handeln in die Öffentlichkeit gelangen.

Bei Krankenakten, OP-Berichten und Personalakten handelt es sich laut Bundesdatenschutzgesetz um personenbezogene Daten, die einem erhöhten Schutzbedarf unterliegen. Verstöße gegen dieses Gesetz werden vom Gesetzgeber unter anderem mit hohen Geldbußen geahndet.

Damit diese sensiblen Daten sicher entsorgt werden, wird die Vernichtung mit mindestens der Schutzklasse 2, Sicherheitsstufe P-4 (bei Informationen in Originalgröße, z. B. Papier) empfohlen. Zuerst gilt es aber gewisse Aufbewahrungsfristen einzuhalten, denn hier gibt es große Unterschiede. So müssen Arbeitsunfähigkeitsbescheinigungen und Überweisungen etc. mindestens ein Jahr aufbewahrt werden, Röntgenaufnahmen, Untersuchungsbefunde mindestens zehn Jahre und Aufzeichnungen über Behandlungen mit radioaktiven Stoffen sowie Aufzeichnungen über Röntgentherapien sogar dreißig Jahre.

Dass trotzdem immer wieder etwas schief läuft, zeigen die bereits angesprochenen Skandale, über die in den Medien berichtet wird. Beispielsweise der Fall einer Hamburger Klinik, die Patientenakten gleich kistenweise im Sperrmüll entsorgt hat. Neben aussortierten Möbeln und Schrott lagerten in dem von der Stadtreinigung aufgestellten Behälter unter freiem Himmel mindestens fünf Kartons, randvoll mit hunderten alten Notfallberichten und Abrechnungsunterlagen mehrerer Hamburger Kliniken. In den Ordnern, die nach Angaben der Klinik zufolge im Schredder landen sollten, befanden sich Diagnosen und Krankheitsvorgeschichten von mehreren tausend Personen, die alle mit vollem Namen und Wohnort in den Berichten vermerkt waren. Briefwechsel mit einem Finanzdienstleister klärten darüber auf, bei welchen Patienten eine Privatinsolvenz vorliegt. Hinweise auf Ehestreitigkeiten fanden sich genauso in den Notfallberichten wie pikante Atteste in der Korrespondenz mit den Krankenkassen, aus der man etwa erfährt, welche Patienten unter einer „affektiven Psychose" leiden (Quelle: www.taz.de/!90750/ abgerufen am 24.06.2014).

Was diesen Kliniken durch Unvorsichtigkeit passiert ist, verletzt zum einen die Datenschutzrechte der betroffenen Patienten, und zum anderen schadet es dem Ruf der Kliniken, denn für ein Krankenhaus sind Patientenakten im Müll einer der größten anzunehmenden „Unfälle".

Es kann aber nicht nur Krankenhäuser und Arztpraxen treffen, besonders gefährdet sind beispielsweise auch Forschungs- und Entwicklungsabteilungen von Unternehmen. Hier muss sogar mit gezielter Wirtschaftsspionage gerechnet werden, die sich schon längst nicht mehr nur auf physisches Datenmaterial beschränkt. Immer wieder tauchen Festplatten und USB-Sticks mit nicht gelöschten Daten auf. Durchwühlte Papierkörbe oder Pannen bei Dienstleistern für externe Datenvernichtung sind in bestimmten Branchen keine Seltenheit.

Dabei sind Unternehmen in der Pflicht, personenbezogene Daten zu schützen, dies ist im BDSG, dem deutschen Bundesdatenschutzgesetz, sowie in den Datenschutzrichtlinien der EU festgelegt. Nach der gesetzlichen Aufbewahrungsfrist müssen die Daten sicher vernichtet werden. Die neue DIN 66399 berücksichtigt nun auch neue Datenträger wie beispielsweise CDs/DVDs, Festplatten sowie elektronische Speichermedien (USB-Sticks etc.). Sie bietet eine umfassende Orientierung für die Vernichtung von „neuen Medien". Zwei zusätzliche Sicherheitsstufen, die der technischen Entwicklung Rechnung tragen, wurden ebenfalls

Intensivseminar mit höchstem Praxisbezug!
23. und 24. September 2014 in Frankfurt/M.

management forum starnberg

IT im Krankenhaus

Krankenhaus-IT im Umbruch: aktueller Stand und Trends

20 JAHRE Management Forum Starnberg

- Wie entwickelt sich die Krankenhaus-IT?
- Elektronische Patientenakte: Vision oder Realität?
- Mobile Patientenakte und Mobilität im Krankenhaus
- Digitale Archivierung von (Patienten)akten
- Pflegedokumentation und Pflegeplanung mit IT
- IT und Medizintechnik wachsen zusammen, aber wie?
- Medizinproduktegesetz und EN 80001:
  Risikomanagement von IT-Produkten in der Medizintechnik
- IT-Netze in Kliniken: aktueller Stand und Entwicklung – worauf ist zu achten

Sonderpreis für Vertreter von Krankenhäusern und Gesundheitseinrichtungen sowie der öffentlichen Hand!

Ihr Seminarleiter:

Prof. Dr. Wolfgang Riedel
IfK Institut für Krankenhauswesen, Braunschweig

Unser Medienpartner:

KTM Krankenhaus TECHNIK + MANAGEMENT

Ihre Praxisreferenten:

Thorsten Schütz
Klinikum Itzehoe

Prof. Dr. Jürgen Stettin
Hochschule für angewandte Wissenschaften, Hamburg

Dr. Pia Wieteck
European Nursing Care Pathways (ENP)

Weitere Informationen und Anmeldung: Tel.: 08151-2719-0
info@management-forum.de · www.management-forum.de/it-kkh

aufgenommen. Die neue Norm definiert neben den reinen Anforderungen an Maschinen zukünftig auch die Prozesse rund um die Datenträgervernichtung.

Eine Studie zeigt: Datenschutz in Deutschland unterschätzt

In Deutschland macht man sich noch wenig Gedanken zu Datendiebstahl und -missbrauch. Das ergab eine Umfrage im Auftrag von HSM, Hersteller von Aktenvernichtern und Festplattenvernichtern. 1005 Unternehmen aus verschiedenen Branchen wurden befragt. Trotz der EU-Datenschutz-Richtlinie, nach denen Verstöße mit Bußgeldern von bis zu 250.000 Euro und sogar Freiheitsstrafen geahndet werden, kam die Studie zu alarmierenden Ergebnissen. 45 Prozent aller Befragten ist nicht bewusst, dass Datendiebstahl aus Mülltonnen zu erheblichem Missbrauch führen kann. Von den befragten Finanzdienstleistern verfügen 23 Prozent über keinerlei interne Richtlinien zu Datenschutz. Rund 11 Prozent der befragten Bankangestellten werfen Blätter zu finanziellen Transaktionen direkt in den Papierkorb.

Aktenvernichter machen vertrauliche Dokumente unleserlich – und das in verschiedenen Sicherheitsstufen. Das Unternehmen HSM stellt beispielsweise Aktenvernichtern in jeder Leistungsgröße her. Neben Papier vernichten selbst kleinere Geräte auch digitale Datenträger mühelos.

Initiative zur Verbesserung des Datenschutzes und der IT-Sicherheit bei niedergelassenen Ärzten und Psychotherapeuten

„Mit Sicherheit gut behandelt“

Schweigepflicht und Vertraulichkeit gehören zu den Basics jeder ärztlichen Versorgung. Gleichwohl sind vielen Behandlern die daraus resultierenden Konsequenzen für den Betrieb der eigenen Praxis kaum bekannt. Spätestens beim Einsatz moderner IT einschließlich der Nutzung von Webdiensten kann dies zum GAU führen. Mit einer Anfang 2014 gestarteten gemeinsamen Initiative des Landesdatenschutzbeauftragten in Rheinland-Pfalz und der dortigen Kassenärztlichen Vereinigung möchte man dieser Gefahr entgegenwirken und Ärzte und Psychotherapeuten für das ungeliebte Thema sensibilisieren. Ein Lagebericht.

Von Michael Heusel-Weiss, Mitarbeiter des LfDI Rheinland-Pfalz, Mainz

Die Anfragen häuften sich im Büro des rheinland-pfälzischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI). Und die Beschwerden auch. Einmal war zu klären, was der Vermieter von Praxisräumen mit einer vollständigen Patientenkartei machen sollte, nachdem sein bisheriger Mieter die von ihm betriebene Arztpraxis geschlossen hatte und einfach verschwunden war. Ein anderes Mal bat ein Patient den LfDI um Unterstützung, nachdem der ihn behandelnde Arzt ihm unter Hinweis auf den Datenschutz die Einsicht in die Behandlungsunterlagen verweigert hatte. Solche und ähnliche Fragestellungen erreichten die Geschäftsstelle des LfDI immer öfter, seitdem dieser im Jahre 2009 die Aufsichtszuständigkeit über die niedergelassenen Ärzte und sonstigen Heilberufler übernommen hatte.

Andere Fragen wurden dagegen nie gestellt: Beispielsweise welche Vorkehrungen zu treffen sind, wenn der Praxisbetrieb auf den Einsatz moderner Informations- und Kommunikationstechnologie umgestellt werden soll. Oder was bei der Einbindung von Dienstleistern zu beachten ist, wenn diese die gerade erst erworbene Praxissoftware betreuen sollen.

Es stellte sich schnell heraus, dass die Zunahme der Anfragen und Beschwerden zur Datenverarbeitung im ärztlichen Bereich einem weit verbreiteten Informationsdefizit bei den Praxisbetreibern geschuldet war. Manchen Ärzten oder Psychotherapeuten war einfach nicht bekannt, welche rechtlichen und technischen Anforderungen an einen sicheren Einsatz von Informationstechnologie im Praxisbetrieb bestehen.

Unklarheiten gab es auch über die Auswirkungen der ärztlichen Schweigepflicht auf den Praxisalltag oder den Umfang der den Patienten zustehenden Einsichtsrechte. Ange-

sichts der damit verbundenen erheblichen Gefährdungspotenziale für die sensiblen Behandlungsdaten und das informationelle Selbstbestimmungsrecht der Patienten regte der LfDI Anfang 2013 gegenüber den Heilberufskammern und der Kassenärztlichen Vereinigung Rheinland-Pfalz (KV RP) ein abgestimmtes Vorgehen zur Verbesserung von IT-Sicherheit und Datenschutz an. Anders als die KV RP konnten sich die Kammern trotz zahlreicher Gespräche und ähnlicher Zielsetzungen bislang einer Kooperation nicht anschließen. Dies ist sehr bedauerlich. Es führte glücklicherweise jedoch nicht zu einem Scheitern des Projektes.

Im Gegenteil: Zusammen mit der KV RP entwickelte der LfDI im Laufe des Jahres 2013 ein tragfähiges Konzept für eine gemeinsame Aktion zur Verbesserung der IT-Sicherheit und des Datenschutzes bei den im Lande ansässigen Ärzten und Psychotherapeuten. Die Umsetzung des Konzeptes mündete in die zum Jahresbeginn 2014 gestartete Initiative „Mit Sicherheit gut behandelt".

Die ambulanten Behandler sollen mit den verschiedenen Bestandteilen der Initiative umfassend bei ihrer Verpflichtung unterstützt werden, im Praxisbetrieb für eine angemessene IT-Sicherheit und einen effektiven Datenschutz zu sorgen. Ziel des Projektes ist es vor allem, allgemein und ohne erhobenen Zeigefinger die Praxisinhaber und deren Mitarbeiter für die Thematik zu sensibilisieren und über bestehende rechtliche Vorgaben zu informieren. Dabei stehen folgende Instrumente zur Verfügung:

— **Website „mit-sicherheit-gut-behandelt.de"**
Kernstück der Initiative ist die zentrale Website „mit-sicherheit-gut-behandelt.de", die thematisch strukturiert umfangreiche Materialien, Handlungsanleitungen, Checklisten und Rechtsgrundlagen zur IT-Sicherheit und den Vorgaben des Datenschutzes bei Betrieb einer Arzt- oder Psychotherapeutenpraxis bereit stellt.

Grund für Aufbau und Gestaltung der Website war die Überlegung, den Praxisbetreibern die bereits zahlreich vorhandenen Inhalte zu der Thematik auf einer einheitlichen digitalen Plattform zusammenzuführen und den Betroffenen damit leichter erschließbar zu machen. Durch die in den einzelnen Seiten integrierten Links haben die Nutzer die Möglichkeit, auch von anderen Stellen in diesem Zusammenhang verfasste Materialien und Serviceangebote zu finden und gegebenenfalls bei ihrem weiteren Vorgehen zu berücksichtigen. Beispiel hierfür sind die von einigen Institutionen entwickelten Selbst-Checks, die es den Praxisinhabern ermöglichen, den aktuellen Sicherheitsstand der eigenen Praxis zu analysieren und gegebenenfalls bestehende Handlungsdefizite zu erkennen.

— Regionale Veranstaltungen
Im Laufe des Jahres 2014 bieten die Kooperationspartner an den vier Standorten der KV RP in Trier, Neustadt/Weinstraße, Mainz und Koblenz halbtägige Informationsveranstaltungen an, in denen ausgewählte Themenfelder zu Fragen der IT-Sicherheit und zum Datenschutz aufbereitet und mit den anwesenden Praxisvertretern diskutiert werden. Es besteht für die Teilnehmer darüber hinaus auch die Möglichkeit, konkrete Anliegen aus ihrem Alltag mit den Referenten zu klären. Mit den regionalen Veranstaltungen wollen die Kooperationspartner einen direkten Dialog mit den Ärzten und Psychotherapeuten aufbauen, der beiden Seiten wertvolle Erkenntnisse im Zusammenhang mit der Beachtung der bestehenden Anforderungen liefern kann.

Bereits die erste Veranstaltung am 21. Mai 2014 in Trier, an der sich auch ein Vertreter der dortigen Bezirksärztekammer beteiligte, übertraf die an sie gestellten Erwartungen deutlich. Mit über 60 Teilnehmern stieß das Informationsangebot bei den Praxisbetreibern und deren Mitarbeitern auf großes Interesse. Die im Programm enthaltenen Kurzreferate führten zu einer lebhaften Diskussion zwischen den Anwesenden. Zahlreiche Rückmeldungen während und nach der Veranstaltung bestätigten die Richtigkeit des seitens der Kooperationspartner insoweit gewählten Ansatzes.

— Beiträge in Publikationsorganen
Mit regelmäßigen Beiträgen zu Einzelthemen aus den Bereichen IT-Sicherheit und Datenschutz sowohl im Mitteilungsorgan der KV RP als auch dem rheinland-pfälzischen Ärzteblatt sollen die im Lande ansässigen Praxisbetreiber immer wieder sensibilisiert und zugleich auf die einzelnen Unterstützungsangebote der Initiative aufmerksam gemacht werden. Hinzukommen noch weitere Sonderpublikationen im Laufe des Jahres. Mit der wiederkehrenden Behandlung datenschutzrechtlicher Inhalte soll deren Vielschichtigkeit und Bedeutung verdeutlicht werden.

— Kontakt mit Systemherstellern und Heilberufskammern
Eine Verbesserung von IT-Sicherheit und Datenschutz bei den niedergelassenen Ärzten und Psychotherapeuten hängt nicht nur von den Anstrengungen der Praxisbetreiber ab: So ist ein datenschutzgerechter Betrieb der Praxissoftware nur dann möglich, wenn die eingesetzten Systeme dies auch funktional zulassen. Ob dies der Fall ist, liegt in der Verantwortung der Systemhersteller. Zudem bilden die Vorgaben des Berufsrechts, insbesondere die ärztliche Schweigepflicht, den Rahmen für die Gestaltung und den Betrieb der Praxen. Deren Auslegung obliegt allerdings den Standesorganisationen.

Aus Sicht der Kooperationspartner ist es deshalb unerlässlich, zur Erreichung des mit der Initiative verfolgten Anliegens auch die Hersteller von Praxisverwaltungssystemen sowie die Heilberufskammern einzubinden. Nur in einem Zusammenspiel aller beteiligten Personen, Institutionen und Stellen können auf diesem Feld Fortschritte erzielt werden. Im Rahmen der Aktion werden deshalb Systemhersteller und Heilberufskammern immer wieder zu Einzelthemen konkret angesprochen.

Beispiel hierfür ist die an die Hersteller herangetragene Anfrage, ob und gegebenenfalls in welchem Umfang die von ihnen bereit gestellten IT-Lösungen in der Lage sind, die in den Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung zu Datenschutz und Datenverarbeitung in der Arztpraxis genannten Anforderungen tatsächlich zu erfüllen. In einem anderen Fall sind die Kooperationspartner an der Position der Berufskammern hinsichtlich einer Nutzung sogenannter Cloud-Dienste durch die Praxisbetreiber interessiert.

Fazit und Ausblick

Welche Erkenntnisse können schon jetzt aus der rheinland-pfälzischen Initiative gezogen werden? Es ist sicherlich beschwerlich, im Umfeld ärztlicher Tätigkeiten breites Interesse für Fragen des Datenschutzes zu wecken. Und es gelingt sicherlich nicht von heute auf morgen, alle in diesem Zusammenhang bestehenden Defizite flächendeckend zu beheben. Darauf kommt es aber letztendlich gar nicht an. Entscheidender ist es vielmehr, die an der ambulanten Heilbehandlung beteiligten Akteure gerade in Zeiten des Web 2.0 von der Notwendigkeit zu treffender Schutzvorkehrungen bei dem Einsatz moderner Informations- und Kommunikationstechnologie zu überzeugen. Und zu verdeutlichen, dass den Patienten im Rahmen der Behandlung zustehende Rechte nicht als generelles Misstrauen gegen das ärztliche Tun zu verstehen sind, sondern Ausdruck des unserer Gesellschaft zugrunde liegenden Rechtsstaates und des ihm angehörenden mündigen Bürgers. Gelingen diese Einsichten, werden sich auch die mit der Initiative beabsichtigten Verbesserungen im Praxisbetrieb schnell genug umsetzen lassen. Die von KV RP und Landesdatenschutzbeauftragten getragene Kooperation möchte hierzu gerne einen Beitrag liefern.

Nähere Informationen zu dem Projekt finden sich auf der Website der Initiative unter www.mit-sicherheit-gut-behandelt.de. Darüber hinaus steht der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz für Fragen zur Verfügung (LfDI RP, Tel.: 06131/208 2449; Mail: poststelle@datenschutz.rlp.de).

HiScout GRC Suite

Herausforderung: Risikomanagement für IT-Netzwerke mit Medizinprodukten im Krankenhaus

Unified Governance, Risk & Compliance, Management

Integriertes IT-Service-, Informationssicherheits- und Risikomanagement im Krankenhaus

www.hiscout.com

HiScout integriert und konsolidiert die Kernanforderungen an ein modernes Informationssicherheits- und Risikomanagement in einem Werkzeug:

1. **IT-Service Portfolio Manager**
   Service-Kataloge und Service-Level gem. ITIL
2. **Information Security Management**
   Informationsrisiken managen nach ISO 27001 und ISO 27799
3. **IT-Grundschutz**
   Informationssicherheit nach BSI 100-1 bis 3, GSTOOL
4. **Risikomanagement medizinischer IT-Netzwerke**
   Risikomanagement-Akte nach IEC 80001-1
5. **Business Continuity Management**
   Notfallprävention und -reaktion nach ISO 22301 und BSI 100-4

Die eigenen Mitarbeiter als Datendiebe?

Insider-Threats verhindern

Es gibt viele Studien, in denen das Vertrauen in die eigenen Mitarbeiter auf den Prüfstand gestellt wird. Vor allem im Bereich der öffentlichen Verwaltung und in Kliniken, in denen sensible Patientendaten von mehreren Personen eingesehen und bearbeitet werden müssen, ist dieses Thema brisant. Etliche wichtige und zum Teil auch höchst sensible Daten existieren nur noch digital, seien es Verträge, Personalakten oder Patientendaten.

Von Christian Sdannowitz, CenterTools GmbH

Viele Unternehmen geben viel Geld aus, um sich gegen Malware, Phishing und andere Bedrohungen durch sogenannte Cyberkriminelle zu schützen. Dabei wird oft übersehen, dass in den eigenen Reihen, bei den eigenen Mitarbeitern ebenfalls Handlungsbedarf besteht. Laut einer Studie von einem amerikanischen Sicherheitsanbieter, die über 500 IT- und Security Manager europaweit zu dem Thema Sicherheit befragt haben, gaben nur 9 Prozent an, sich vor der Bedrohung der eigenen Mitarbeiter sicher zu fühlen.

Es müssen nicht immer die eigenen Mitarbeiter sein, auch Angestellte über Fremdfirmen haben meistens Zugriff auf mehr Daten, als sie eigentlich haben sollten. In Kliniken waren es zu Beginn einst nichtmedizinische Leistungen, die outgesourct wurden, nach und nach wurden aber auch medizinische Bereiche wie Labor oder Radiologie ausgelagert.

Ein weiteres Beispiel: Was passiert, wenn einem Mitarbeiter gekündigt wird? Ist dann sichergestellt, dass dieser Mitarbeiter keine sensiblen Firmendaten mitnimmt? Im Fall Snowden ist sehr klar zu erkennen, welche Auswirkungen es haben kann, wenn Mitarbeiter vertrauliche Daten mitnehmen.

Das muss nicht absichtlich geschehen: Ein Arzt kann sein mobiles Endgerät mit sensiblen Daten am Flughafen oder im Taxi liegenlassen. Vergangene Vorfälle solcher Art zeigen, dass der Image- und Reputationsverlust sehr hoch sein kann und zum Teil drakonische Strafen drohen. Denn bei Weitergabe oder Veröffentlichung von Patientendaten drohen den Ärzten und Kliniken Freiheitsstrafen oder Geldstrafen (§ 203 StGB). Auch der finanzielle Verlust ist enorm: Laut der Ponemon Studie „Cost of a Data Breach 2013“ müssen Unternehmen im öffentlichen Bereich mit Kosten von 93 Euro pro verlorenem Datensatz rechnen. Hier sollte das Unternehmen dem Mitarbeiter in puncto Sicherheit immer einen Schritt voraus sein.

Was hilft gegen die sogenannte Bedrohung von innen?

Ob interne Festplatten, externe Datenträger oder Daten in der Cloud: Sensible Unternehmensdaten müssen verschlüsselt werden. Optimal ist es, wenn neben der Verschlüsselung noch eine Daten- und Schnittstellenkontrolle in die Sicherheitslösung integriert ist, die festlegt, welche Anwendung oder welche Datei von wem auf welchem Gerät genutzt werden darf. Diese Komponenten bieten einen optimalen Rundumschutz, der auch den Grundstein für eine ISO-27001 Zertifizierung bietet, was erfolgreich beispielsweise am Universitätsklinikum Hamburg-Eppendorf zu sehen ist. Natürlich ist es hilfreich, wenn die eingesetzte Sicherheitssoftware strenge Richtlinien oder Betriebsvereinbarungen abbilden kann.

Des Weiteren sollten sogenannte Rechtemodelle integriert werden, die zentral konfigurierbar und höchst granular einstellbar sind. Somit kann beispielsweise dem entlassenen Mitarbeiter jegliche Kopie sensibler Daten untersagt werden, oder der Zugriff bis zu seinem endgültigen Ausscheiden verweigert werden.

In vielen Krankenhäusern und größeren Einrichtungen hat sich die Verwendung von Thin Clients erfolgreich etabliert. Aber auch Thin Clients verfügen über USB-Ports, an denen Anwender externe Laufwerke anschließen können, die dann „remote“ im Hostbetriebssystem eingebunden werden. Sofern Geschäftsprozesse deren Nutzung erfordern, sollten Regeln für Schnittstellen- und Dateimanagement sowie Verschlüsselung auch in der virtuellen Umgebung greifen.

Doch zuvor sollten Unternehmen wissen, welche Schnittstellen im Firmennetzwerk existieren, und welche Datenträger und externen Geräte angeschlossen werden. Hierzu bieten viele Hersteller einen kostenlosen Device-Scanner an, der zum Teil überraschende Ergebnisse liefert.

Gefahr durch Administratorzugänge

Grundsätzlich besteht dann immer noch die Gefahr durch administrative Zugänge. Etwa ein Drittel der Unternehmen gaben an, dass sie eine sehr große Gefahr durch die privilegierten Nutzerkonten, wie sie etliche Administratoren besitzen, sehen. Es ist auch erwiesen, dass Hacker gezielt Administratoren oder Anwender mit privilegierten Rechten angreifen, um an weitere Konten und Kennwörter zu gelangen.

Viele Unternehmen wissen nicht, wie sie die sensiblen Daten gegen Mitarbeiter und vor allem auch Administratoren schützen können. In diesem Fall besteht die Lösung darin, mit zugewiesenen Zertifikaten die Rechtevergabe zu verwalten. Dabei sollte berücksichtigt werden, dass wichtige Aufgaben wie z.B. die Durchführung einer Datensicherung oder das Ändern von Berechtigungen nicht beeinflusst werden. Hierzu wird dann nur die Datei verschlüsselt, die Zugriffsberechtigungen, welche über das Betriebssystem eingerichtet wurden, bleiben dabei unverändert.

Die Rolle des Reporting

Eine zukunftsfähige Sicherheitslösung ist optimal darauf ausgerichtet, sowohl die immer professioneller werdenden Angriffe von außen abzuwehren als auch Aktionen im Inneren zu überwachen und gegebenenfalls zu verhindern. In vielen Unternehmen wissen die Verantwortlichen auch nicht, wo die Ursachen liegen oder von welchen Arbeitsplätzen potenzielle Gefahren drohen.

Hier steht die Reporting-Funktion im Mittelpunkt, die am besten über dynamisch erzeugte Abfragen die Verwendung von Wechseldatenträgern, Geräten oder den gesamten Datentransfer überwacht. Im Notfall sollte die eingesetzte Software einen Vorfall analysieren und aus verschiedenen Blickwinkeln mögliche Datenlecks rekonstruieren können. Einfache Sicherheitssoftware kann feststellen, welche Ports offen sind und die Möglichkeiten eingrenzen.

Optimal ist es, wenn die Software aufzeigt, von welchem Computer eine bestimmte Datei auf welchen externen Datenträger kopiert wurde (Seriennummer), ob sie umbenannt wurde oder ob noch weitere Daten übertragen wurden. Der Weg, den die Datei firmenintern ging, und auf welchen Weg sie die Firma verlassen hat, ist dabei entscheidend.

Sensibilisierung

Eine andere Herausforderung besteht neben der technischen Absicherung der sensiblen Daten auch in der Schulung und Sensibilisierung der eigenen Mitarbeiter. Das Ponemon Institut analysierte bei 277 Firmen weltweit die Folgen eines Datenverlustes. Dabei wurde festgestellt, dass 36 Prozent der analysierten Vorfälle durch Mitarbeiter fahrlässig verursacht wurden.

Zurecht sehen rund 74 Prozent der befragten IT-Manager der Vormetric Studie Handlungsbedarf. Manche Anbieter von Sicherheitssoftware bieten an, das Sicherheitsbewusstsein der Mitarbeiter durch gezielte, in die Software integrierte Kampagnen zu schulen. Somit kann beispielsweise bestimmt werden, dass falls ein Anwender einen USB-Stick anschließt, er im ersten Schritt über mögliche Sicherheitsrisiken aufgeklärt wird, bevor er den Stick verwenden darf.

Zusätzlich kann eine transparente Darstellung über die Funktionen der eingesetzten Sicherheitssoftware abschreckend wirken, wenn zum Beispiel die Mitarbeiter wissen, dass von allen abgehenden Dateien Schattenkopien gespeichert werden.

Fazit

In Kliniken spielt der Faktor Zeit und Effizienz eine entscheidende Rolle. Deshalb ist es essenziell, dass die Ärzte und das Krankenhauspersonal durch die eingesetzte Sicherheitslösung nicht behindert oder aufgehalten werden. Die Sicherheitslösung sollte möglichst unbemerkt im Hintergrund agieren. Ebenfalls sollten die höchst granularen Einstellungen, die vorgenommen wurden, in einer durchdachten Administrationsoberfläche optimal angezeigt werden, um den Implementierungs-Aufwand möglichst gering zu halten.

Abschließend kann man festhalten, dass gegen die „Insider Threats“ viele Faktoren zusammenspielen, um einen umfassenden Schutz bestmöglich zu gewährleisten. Als Basis dient die Verschlüsselung der Daten, bei der neben Festplatten ebenso USB-Sticks, eSATA-Festplatten oder gebrannte CDs /DVDs mit zertifizierten Verfahren verschlüsselt werden sollten.

Die Verschlüsselung sollte im Zusammenspiel mit einer Applikations- und Schnittstellenkontrolle eingesetzt werden, bei der über Rechtevergaben, Whitelist-Regeln und Zertifikate festgelegt werden kann, wer welche Datei sehen oder welche Anwendung ausführen kann und/oder darf. Deshalb sollte auf der Agenda eines jeden Geschäftsführers beziehungsweise Security Managers eine Lösung stehen, die diese oben genannten Punkte vereint.

Die Firma CenterTools zum Beispiel bietet mit ihrer Lösung DriveLock eine Security-Lösung an, die einfach zu implementieren und durch ihren mehrschichtigen Aufbau höchst granular einstellbar ist. Dabei verbindet DriveLock die Eigenschaften der Verschlüsselung mit integrierter Datei- und Schnittstellenkontrolle, integriertem Antivirus und einer Sicherheitskampagne, die die Mitarbeiter individuell sensibilisieren kann. ■

Komplettlösungen sichern Praxis-IT ab

Praxissysteme schützen, Patientendaten sichern

Cyberkriminalität und systematische Spionage sind mittlerweile leider ein Alltagsproblem. Alle zwei Sekunden wird weltweit ein Schadprogramm ins Netz gestellt. Alle 30 Sekunden wird eine Identität im Web gestohlen. Das Netz kennt keine Ländergrenzen. Die Komplexität der Viren und die Angriffe aus dem Internet nehmen dramatisch zu. Daher ist es heute wichtiger denn je, sich möglichst umfassend zu schützen.

Von Dirk Roeder, CGM Deutschland AG, Geschäftsbereich telemed

Gerade im Gesundheitswesen hat Datenschutz oberste Priorität. Grundsätzlich gilt die ärztliche Schweigepflicht gem. § 203 Strafgesetzbuch. Dies gilt auch für die Online-Übertragung von Sozialdaten/ Patientendaten sowie den Schutz der Praxis-EDV vor Zugriffen aus dem Internet. Die ärztliche Schweigepflicht ist von grundlegender Bedeutung für das Vertrauensverhältnis zwischen Arzt und Patient sowie der Wahrung von Patientengeheimnissen. Eine Verletzung dieser Grundlagen kann mit einer Geld- oder Freiheitsstrafe geahndet werden. Zur sicheren Online-Kommunikation sind vor allem das Bundesdatenschutzgesetz (BDSG) sowie die Datenschutzempfehlungen der Kassenärztlichen Bundesvereinigung (KBV) und der Bundesärztekammer (BÄK) richtungsweisend. Besondere Relevanz erfahren die Datenschutzvorschriften im Hinblick auf die ärztliche Dokumentationspflicht.

Datenschutzkonforme Übertragung von Patientendaten

Das Internet als Kommunikationsplattform in Praxen kann nicht mit dem Verhalten von Privatnutzern verglichen werden. Aus straf- und haftungsrechtlichen Gründen sind besondere Datenschutzvorkehrungen in der Praxis unumgänglich.

Den optimalen Schutz bietet die Daten- und E-Mail-Übertragung in einem geschlossenen Intranet wie zum Beispiel über die DSL, SDSL, VDSL, ISDN oder UMTS Vollzugänge von telemed. Hier erfolgt die Router-Einwahl der Praxis direkt in das Intranet, wo die Daten sicher und datenschutzkonform übertragen werden. Durch den Einsatz von zentralen Sicherheitsmechanismen wie Firewalls, Proxy-Server, Virenscanner, NAT ist die einzelne Praxis für Angreifer aus dem Internet nicht sichtbar.

Für den Zugriff ins Internet kann die Praxis zwischen drei telemed-Sicherheitszonen wählen:

— X-Zone
Die X-Zone bietet der Praxis den Zugriff auf Dienste der Kassenärztlichen Vereinigungen (KVen) beziehungsweise der Hausärztlichen Vertragsgemeinschaft (HzV) und der Kassenzahnärztlichen Vereinigungen (KZV) wie zum Beispiel die Online-Abrechnung und den eDMP-Versand. Weiter können telemed Mehrwertdienste wie der SMS-Versand, die gesicherte E-Mail-Übertragung, der Versand von eArztbriefen genutzt werden. Die Übertragung erfolgt hierbei geschützt im telemed-Intranet. Der Zugang zum Internet ist in dieser Sicherheitszone nicht möglich.

— S-Zone
Die S-Zone bietet den gleichen Leistungsumfang wie die X-Zone. Zusätzlich besteht hier die Möglichkeit, dedizierte, auf Sicherheit geprüfte fachliche Internetseiten aufzurufen (Whitelist). Zu diesen Seiten gehören zum Beispiel Seiten von Krankenkassen, Kassenärztlichen Vereinigungen, Arztinformationssystemherstellern, medizinische Inhalte.

— I-Zone
Auch die I-Zone bietet den Praxen die sichere Nutzung von Diensten der KVen beziehungsweise der HzVen und der KZVen sowie der telemed-Mehrwertdienste. Im Gegensatz zu den Varianten I und S hat der Teilnehmer hier jedoch die Möglichkeit, einen überwiegenden Teil aller Internetseiten aufzurufen, wobei potenziell gefährliche Webseiten gesperrt

sind (Blacklist). Die Blacklist wird seitens telemed permanent gepflegt und aktualisiert, was mehr Komfort und Sicherheit für die Praxen bedeutet.

Neben der Datenübertragung mittels Direkteinwahl in ein geschlossenes Intranet ist – zum Beispiel für Praxen, die bereits über einen herkömmlichen Online-Zugang verfügen – die Datenübertragung mittels eines Virtual Private Network (VPN) möglich. Hierbei erfolgt über einen bestehenden Online-Zugang der Praxis via Hardware- oder Software VPN die Einwahl in das Intranet, wo die sichere Datenübertragung erfolgt. Der Zugang ins Internet erfolgt dabei allerdings über den vorhandenen Provider und nicht über die Schutzmechanismen eines Intranets mit Direkteinwahl. Hierdurch besteht für die Praxis ein erhöhtes Risiko für Angriffe aus dem Internet über den vorhandenen Provider. Die Direkteinwahl über ein geschlossenes Intranet ist daher datenschutzrechtlich der Datenübertragung via VPN vorzuziehen.

KV-SafeNet

KV-SafeNet ist die hardwarebasierte, hochsichere Anbindungsvariante an das sogenannte „Sichere Netz der KVen“ (SNK), welche von den Landesdatenschützern zur Kommunikation von Sozial- und Patientendaten empfohlen wird. Auch hier ist die Anbindung per Direkteinwahl in ein Intranet als auch die Datenübertragung via VPN möglich. Über KV-SafeNet können unter anderem die seit dem ersten Quartal 2011 verpflichtende Online-Abrechnung sowie eDMP-Daten und eArztbriefe datenschutzkonform übertragen werden.

Zur Installation der KV-SafeNet-Zugänge in den Arztpraxen ist vor allem die Vor-Ort Unterstützung - auch im Supportfall - wichtig. Das Unternehmen telemed bietet Arztpraxen ein bundesweites KV-SafeNet geschultes und zertifiziertes Servicepartnernetz für Konfiguration, Installation und Wartung der Zugänge und Endgeräte direkt vor Ort.

Online-Rollout zur Erprobung der ersten Stufe der Telematik-Infrastruktur

Neben KV-SafeNet wird in Deutschland aktuell der sogenannte Online-Rollout der Telematik-Infrastruktur in zwei Testregionen (Nord-West und Süd-Ost) erprobt. Der Begriff „Telematik“ ist eine Kombination der Wörter „Telekommunikation“ und „Informatik“. Es handelt sich hierbei um die Vernetzung der IT-Systeme von Arztpraxen, Apotheken, Krankenhäusern und Krankenkassen und ermöglicht so einen systemübergreifenden Austausch von Informationen.

Die Telematik-Infrastruktur ist ein geschlossenes Netzwerk, zu dem man nur mit Heilberufsausweis und Gesundheitskarte Zutritt erlangt. Sie wird konzipiert und eingeführt von der „gesellschaft für Telematikanwendungen der Gesundheitskarte mbH“ (gematik), einer Organisation, die von den Spitzenverbänden der Leistungserbringer und Kostenträger des deutschen Gesundheitswesens gegründet wurde.

Zentrales Thema der Konzeption der Telematikinfrastruktur ist, dass sie bestehende Informationsgrenzen im Gesundheitswesen überwindet. Die ärztliche Schweigepflicht und das Recht auf informationelle Selbstbestimmung bleiben jederzeit gewahrt.

Aktuell wird die Online-Infrastruktur zur Vernetzung der Teilnehmer im Gesundheitswesen erprobt. Diese soll nach der eingehenden Erprobung mit umfassender Evaluation, die 2016 abgeschlossen sein soll, bundesweit ausgerollt werden.

KV-SafeNet dient der Anbindung der Leistungserbringer an das sichere Netz der Kassenärztlichen Vereinigungen (KVen)

Für die Testregion Nord-West erhielt im Dezember 2013 die CompuGroup Medical AG im Konsortium mit Strategy& und KoCo Connector von der gematik den Auftrag für den Online-Rollout zur Erprobung der ersten Stufe der Telematik-Infrastruktur in der Testregion Nord-West (Rheinland-Pfalz, Nordrhein-Westfalen, Schleswig-Holstein).

Der Geschäftsbereich telemed stellt in dieser Testregion insbesondere die Netzinfrastruktur bereit. Weiter wird der Support, basierend auf den bereits im Bereich KV-SafeNet bewährten Strukturen, gewährleistet. Ausschreibungsgegenstand für die Testregion war die Ausstattung der teilnehmenden Heilberufler (Ärzte, Zahnärzte, Psychotherapeutenpraxen und Krankenhäuser) mit allen für die Anbindung an die Telematikinfrastruktur notwendigen Komponenten und Diensten (bspw. Konnektoren von KoCo Connector, Kartenterminals von Ingenico Orga, VPN-Zugangsdienste) sowie deren Entwicklung, Aufbau und Betrieb.

Sichere Heimarbeit weltweit via USB-Stick oder App

Wichtig ist, dass alle Mehrwertdienste, die der Arzt bisher genutzt hat, in der Telematik-Infrastruktur und dem KV-SafeNet weiter

reibungslos funktionieren. Dies gilt insbesondere auch für die Heimarbeit, denn Arzt zu sein ist nicht nur Beruf, sondern Berufung. So arbeiten viele Ärzte auch nach Praxisschluss von zu Hause aus weiter oder möchten auf Schulungen, Fortbildungen und unterwegs jederzeit über den aktuellen Stand und wichtige Ereignisse in ihrer Praxis informiert sein.

Dies ist zum Beispiel über die telemed Mobile Praxis Center und Mobile Praxis Tablet möglich. Über eine beliebige Internetverbindung wird via USB-Stick (Desktop-PCs, Notebook) oder App (Tablet-PCs) auf die Arbeitsplatz-PCs der Praxis zugegriffen. Ein spezieller Dienst ermöglicht hierbei aus der Praxis eine gesicherte VPN-Verbindung zum zentralen Gateway im telemed-Netz. Der USB-Stick oder die App bauen im Gegenzug von extern ebenfalls eine passwortgeschützte VPN-Verbindung zum zentralen Gateway im telemed-Netz auf.

Über diese Verbindung wird remote auf das Arztinformationssystem in der Praxis zugegriffen. Dies ermöglicht dem Nutzer das Lesen und Ändern von Daten oder Einlesen elektronischer Gesundheitskarten direkt im Arztinformationssystem in der Praxis sowie das Drucken von Daten aus der Praxis auf dem externen Computer.

Zusätzlich bietet die Tablet Variante via App dem Teilnehmer eine Touch-Steuerung seines Praxis-PCs. Auch die im täglichen Einsatz viel genutzten Funktionstasten und Shortcuts kann er nutzen, denn diese sind in der virtuellen Tastatur hinterlegt.

Viren- und Malware-Schutz für Praxis-PCs

Ein besonderes Augenmerk ist auf den Virenschutz der Praxis PCs zu legen. Alle einschlägigen Datenschutzempfehlungen im Gesundheitswesen, wie die der KBV und BÄK sowie die „Sicherheitsanforderungen für SafeNet-Arbeitsplätze“, raten den Praxen dringend zur Installation einer lokalen Virenschutzsoftware.

Aufgrund der aktuellen Bedrohungslage ist es sinnvoll, Virenschutzlösungen einzusetzen, die neben den lokalen Virendefinitionen auch auf eine Cloud-Prüfung zurückgreifen. So ist zum Beispiel mit dem telemed Protect Virenschutz jeder Teilnehmer im Gesundheitswesen optimal geschützt. Neben einem umfassenden Antiviren-Schutz, einer Personal-Firewall sowie Anti-Malware-, E-Mail- und Download-Schutz zeichnet sich telemed Protect vor allem durch seinen Echtzeit-Schutz durch Zugriff auf ein zentrales, permanent gemanagtes Bedrohungsverzeichnis aus.

Der telemed Protect Virenschutz lässt sich einfach installieren bei gleichzeitig minimiertem Ressourcenverbrauch der Arbeitsplatz PCs in der Praxis. Optimierte Update-Technologien sorgen für einen geringen Bandbreitenbedarf. Optional können aktiv Informationen über einen Virenbefall abgerufen werden. Ebenso können standardisierte oder spezielle Reports, wie zum Beispiel Statusreports oder Erkennungsreports, angezeigt werden. All dies spart in der täglichen Praxisarbeit Zeit und Geld – und sichert wertvolle Daten.

Als Ergänzung zum lokalen Virenschutz bietet zum Beispiel das Produkt „telemed Protect Center“ zusätzlich einen zentralen Online-Virenscanner für Browserinhalte. Dieses erkennt und entfernt Viren, bevor diese auf den Praxisarbeitsplatz gelangen. Der durch telemed zentral im Intranet gemanagte Schutz benötigt keine gesonderte Installation und verbraucht keinerlei Ressourcen der Arbeitsplatz PCs.

Schutzschild für die Praxis

Seit Februar 2013 gelten die neuen Paragrafen 630a bis 630g des Bürgerlichen Gesetzbuches, die die Rechte der Patienten und ihre Position im Gesundheitssystem stärken. Für die behandelnden Ärzte bringt das vor allem mehr Pflichten: Auch die elektronische Dokumentation in der Praxis muss veränderungsfest sein. Das heißt, Löschungen oder Änderungen müssen jederzeit nachvollzogen werden können, und das Original muss erhalten bleiben. Durch die strengeren Vorgaben gewinnen rechtskonforme Praxissysteme und der Schutz vor Datenmissbrauch stark an Bedeutung.

Die standardisierte Lösung CGM MEDGUARD zum Beispiel macht die Praxis zur gesicherten Umgebung: Nach der Installation von Hard- und Software ist sie gegen böswillige Hacker-Angriffe abgeschirmt, verfügt über einen gesicherten Online-Zugang und Patientendaten sowie Dokumente werden qualifiziert elektronisch signiert und somit zuverlässig vor Manipulation und Datendiebstahl geschützt.

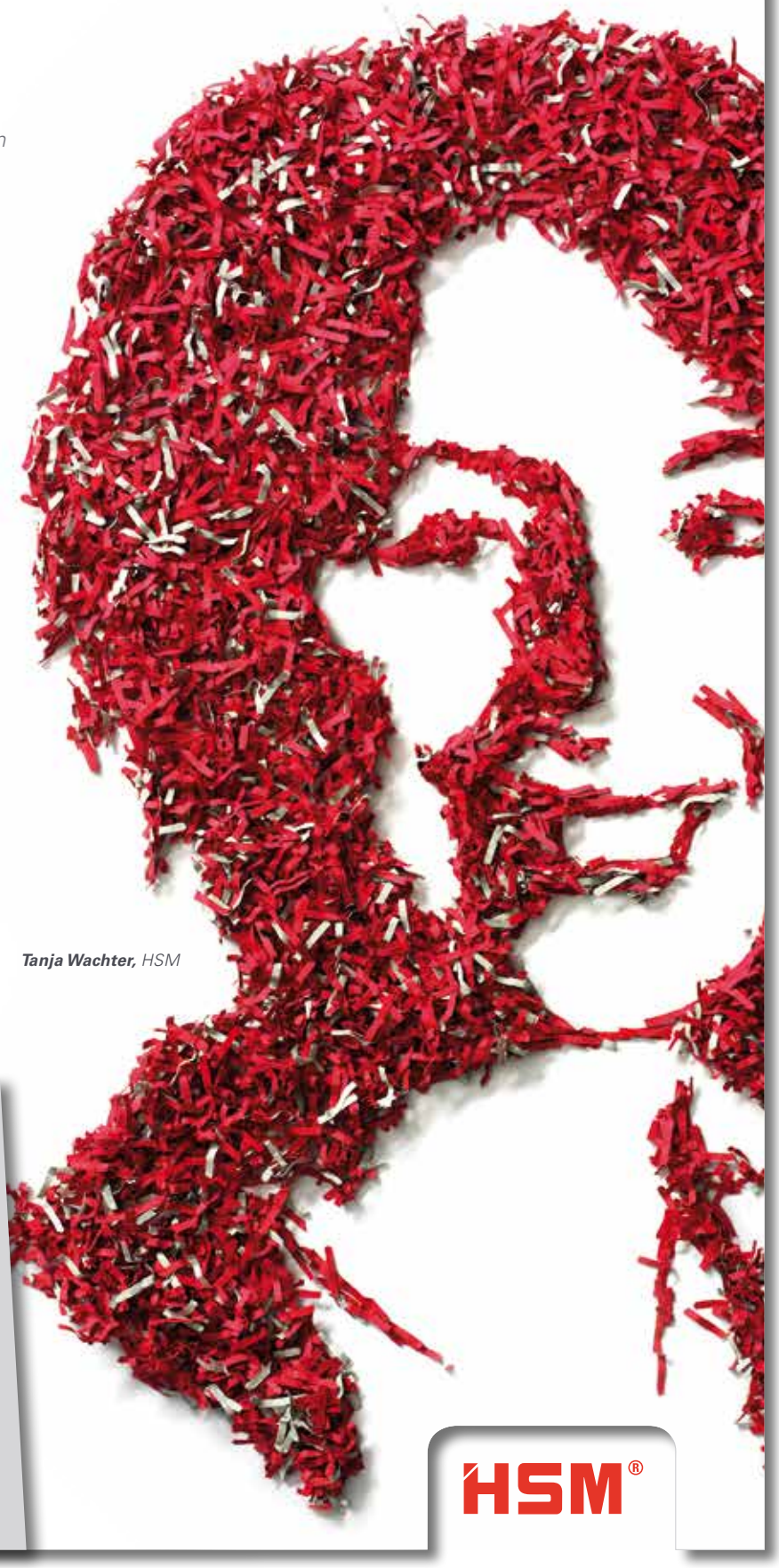
HSM – Mehr als ein Shredder.

Patientendaten auf Papier, Chipkarte oder Festplatte sind besonders sensible Daten. Im Fachjargon werden sie personenbezogene Daten mit erhöhtem Schutzbedarf genannt.

Denken Sie deshalb daran, die Datenträger in einem passenden Aktenvernichter zu schreddern, wenn sie nicht mehr benötigt werden. Zum Beispiel in Sicherheitsstufe P-4 oder P-5.

Dann sind Sie sicher, dass Daten Ihrer Patienten gemäß DIN 66399 vernichtet sind.

Mehr Information erhalten Sie auf www.hsm.eu



***Tanja Wachter,** HSM*

Jetzt neu im App Store!

*Die neue HSM **ShredEffect** App: Verwandeln Sie Ihr Foto in ein Schnipselportrait. Sie werden sehen, wie gut Ihnen Datenschutz steht.*

HSM®

Sichere Daten in Arztpraxen und Kliniken

Kein gläserner Patient

Patientendaten sind sogenannte „personenbezogene Daten natürlicher Personen", die dem besonderen Schutz des Bundesdatenschutzgesetzes (BDSG) unterliegen. Das BDSG schreibt unter anderem technische Maßnahmen vor, die zum Schutz der Daten zwingend eingeführt werden müssen. Warum verlassen sich dennoch viele Organisationen im Gesundheitswesen beim Datenschutz lediglich auf ihre Mitarbeiter?

Von Sergej Schlotthauer, EgoSecure GmbH

Alle Organisationen der Gesundheitsbranche – also auch Kliniken und Praxen - arbeiten grundsätzlich mit Daten, die besonders schützenswert sind. Zum einen enthalten sie sehr persönliche Informationen über die Gesundheit der Patienten, zum anderen handelt es sich stets um Daten von natürlichen Personen, die deshalb dem Schutz durch das Bundesdatenschutzgesetz (BDSG) unterstehen. Alle diese Daten liegen heutzutage in digitaler Form vor und werden durch die EDV verarbeitet, transportiert und gespeichert.

Eigentlich sollte man meinen, dass gerade Heathcare-Organisationen besondere Maßnahmen ergreifen, um diese sensiblen Daten zuverlässig zu schützen. Leider sieht es in der Realität aber oft ganz anders aus. Die Datenschutzmaßnahmen in Klinken und Praxen hinken denen, die etwa in Industrieunternehmen zum Know-how-Schutz betrieben werden, deutlich hinterher. Dabei verlangt das BDSG von jeder Organisation, die personenbezogene Daten von natürlichen Personen erhebt, verarbeitet und speichert, dass diese ganz konkrete Maßnahmen einführt.

Hierzu zählen neben zahlreichen organisatorischen auch technische Maßnahmen, wie beispielsweise Zugriffskontrolle, Protokollierung oder Verschlüsselung. Diese sind explizit im § 9 BDSG und in der entsprechenden Anlage beschrieben. Gehen Daten verloren, verlangt das Gesetz auch für Klinken und Praxen imageschädigende Veröffentlichungspflichten und hohe Bußgelder – ganz zu schweigen von den Schadensersatzansprüchen, die Betroffene unter Umständen geltend machen. Außerdem besteht die Gefahr, dass die Patienten in andere Praxen oder Kliniken abwandern.

Vertrauen und Policies reichen nicht

Dennoch werden technische Datenschutzmaßnahmen im Gesundheitsbereich ein wenig stiefmütterlich behandelt. Vielleicht liegt das zum Teil darin begründet, dass Mitarbeiter dieser Branche grundsätzlich einer besonderen Berufsethik unterliegen, in der Verschwiegenheit und Vertrauen eine besondere Rolle spielen. Aber reicht es aus, Datenschutz nur über Vertrauen in die Mitarbeiter zu regeln? Der Gesetzgeber verneint diese Frage deutlich, denn er schreibt ganz konkrete Maßnahmen vor. Aber auch ohne den Einfluss von Justitia muss man im Sinne der Patienten deutlich davon abraten, nur auf Vertrauen zu bauen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist in seinem „Leitfaden Informationssicherheit – Version Februar 2012" ausdrücklich darauf hin, dass viele Datenverluste nicht durch Vorsatz, sondern sehr oft durch Versehen oder Übereifer, gepaart mit mangelndem Problembewusstsein, zustande kommen.

Diese Tatsache zeigt, dass die Aufstellung eines Regelwerkes für Verhaltensweisen im Umgang mit Daten (Policies) alleine nicht ausreicht, um Verluste von Patientendaten zuverlässig zu verhindern. Werden Policies gut kommuniziert und ausreichend geschult, kann man das mangelnde Problembewusstsein sicherlich gut eindämmen, gegen Versehen oder Übereifer schützen sie jedoch nicht. Somit wird es praktisch eine Frage der Fürsorgepflicht für die Mitarbeiter, technische Maßnahmen in der Datensicherheit einzuführen, die sowohl bei fahrlässigem als auch vorsätzlichem Handeln Schäden vermeiden.

Der Weg zu mehr Datensicherheit

Ein erster Schritt in die richtige Richtung ist festzulegen, welche Personen welche Datenwege benutzen dürfen. Gerade bei Patientendaten ist es gesetzlich vorgeschrieben, dass nur jene Angestellten Zugriff erhalten, die eine entsprechende Schulung im Umgang mit personenbezogenen Daten genossen und eine Geheimhaltungserklärung unterschrieben haben (vgl. Zugriffskontrolle Anlage § 9 Satz 1 BDSG). Technisch lassen sich mit einer Access-Control-Lösung zentral die Berechtigungen von Benutzern einstellen. Gute Lösungen bieten sogar Verwaltungsmöglichkeit für Schulungsnachweise und Geheimhaltungserklärungen an. Niemand ohne Berechtigung kann somit sensible Daten „aus Versehen" verlieren, denn er kann überhaupt nicht darauf zugreifen.

Im nächsten Schritt gilt es festzulegen, welcher Umgang mit den Daten für die berechtigten Mitarbei-

ter im Hinblick auf ihre Arbeit Sinn macht. Sicherlich wird es besonders gefährlich, wenn digitale Daten etwa mit USB-Sticks transportiert werden müssen oder auch mobile Geräte wie Laptops zum Einsatz kommen. Daher sollte der Kreis derer, die Daten außerhalb des IT-Netzwerkes transportieren dürfen, sinnvoll eingeschränkt werden. Lediglich Mitarbeiter, die im Rahmen ihrer Tätigkeit eine besondere Flexibilität benötigen, sollten die Berechtigung bekommen. Außerdem erscheint es sinnvoll, nur die Nutzung ganz bestimmter Geräte, die beispielsweise über eine sichere Verschlüsselungslösung verfügen, zu erlauben. Bei der Umsetzung dieser Maßnahmen helfen Device-Management-Lösungen.

Jegliche vertrauliche Daten, die transportiert werden – egal über welches Gerät - müssen verschlüsselt werden. Für Laptops sollte mindestens eine Folder-Verschlüsselung, am besten aber eine komplette Festplattenverschlüsselung, vorhanden sein. Bei der Implementierung einer Verschlüsselung sollte eine Methode gewählt werden, die von den Mitarbeitern auch tatsächlich genutzt wird. So sind klassische Partitionsverschlüsselungen (auch Containerverschlüsselungen genannt) vielleicht sicher, sie werden aber im Praxisalltag leider oft umgangen.

Das liegt daran, weil sie zusätzliche Arbeitsschritte, wie die Definition und das Anlegen von Containern und ein Passwort-Management, erforderlich machen. Zeit ist im Alltag von Kliniken und Praxen immer sehr knapp bemessen und sollte in erster Linie den Patienten zugute kommen. Daher sind Verschlüsselungslösungen, die sich vollkommen im Hintergrund um sämtliche Sicherheitsaspekte kümmern und keine zusätzlichen Arbeitsschritte nötig machen, deutlich besser als Partitionsverschlüsselungen.

Zwingend erforderlich und auch vom Gesetzgeber verlangt, ist eine Protokollierung. Sie macht Datenverluste nachvollziehbar. Schnell regt sich jedoch der Verdacht, dass Mitarbeiter dadurch ausspioniert werden. Doch auch das untersagt der Gesetzgeber – es muss also eine Lösung her, die beide Anforderungen erfüllen kann. Sie sollte so konzipiert sein, dass sie nur dann Informationen über die persönlichen Tätigkeiten von Mitarbeitern im Datenumgang preisgibt, wenn ein Schaden oder gar ein Gesetzesverstoß eingetreten ist und deshalb auch der Arbeitnehmervertreter einer Einsicht in die Protokollierung zustimmt. Dies könnte dann zum Beispiel durch die Vergabe von mehreren Passwörtern, die nur gemeinsam funktionieren, gewährleistet werden.

Mehr Sicherheit für Patientendaten

Access Control, Device Management, verschiedene Verschlüsselungen für unterschiedliche Datenwege und Protokollierung als Mindestanforderung für einen effektiven und gesetzeskonformen Datenschutz. Da regt sich schnell der Verdacht, dass die Einführung technischer IT-Sicherheitsmaßnahmen ein Großprojekt ist, das kaum eine Klinik und schon gar keine Praxis leisten kann.

Oft wird die IT-Administration lediglich von IT-affinen Mitarbeitern übernommen, deren Hauptaufgaben aber eigentlich im medizinischen oder pflegerischen Bereich liegen. Diese könnten ein IT-Großprojekt ohne kostspielige externe Unterstützung überhaupt nicht stemmen. In der Tat ist das oft der Hauptgrund, warum trotz aller Risiken und Gesetze von der Einführung technischer Datenschutzmaßnahmen abgesehen und weiterhin auf das reine Vertrauen gesetzt wird.

Mittlerweile existieren jedoch voll integrierte Gesamtlösungen für alle aufgeführten Funktionen – zum Beispiel EgoSecure Endpoint. Solche Lösungen arbeiten mit nur einer Datenbank und einer zentralen Management-Konsole, was die Installation, die Interaktion der Funktionen und die Administration deutlich vereinfacht. Die komplette Installation aller Funktionen kann je nach Gegebenheiten in weniger als einer Stunde ohne externe Hilfe erfolgen. Danach besteht bereits ein sehr weitreichender Basisschutz. Die weiteren Feineinstellungen, wie etwa die Vergabe der Berechtigungen, finden dann über die zentrale Management-Konsole statt. Diese ist weitgehend intuitiv zu bedienen und erfordert deshalb keine zeitraubende Schulung – eine einfache Einweisung reicht aus.

Auf den Endgeräten ist ein sogenannter Agent installiert, der den Benutzer transparent über die entsprechenden Sicherheitseinstellungen und Einschränkungen mit klaren Botschaften informiert. Die meisten Sicherheitsfunktionen laufen jedoch vollständig im Hintergrund ab und werden vom Benutzer gar nicht wahrgenommen. Diese benutzerfreundliche Architektur der Lösung verringert Anrufe am Help-Desk deutlich und bedeutet keine zusätzliche Belastung für den Mitarbeiter, der mit der Administration betraut ist.

Fazit

Patientendaten unterliegen einem besonderen Schutz und sind durch das BDSG geschützt. Das BDSG schreibt konkrete Maßnahmen zum Schutz der Daten vor, die teils organisatorischer und teils technischer Natur sind. Die Einführung technischer Maßnahmen muss heutzutage kein Großprojekt mehr sein, das Kliniken und Arztpraxen überfordert. Moderne Lösungen sind einfach zu installieren, intuitiv zu administrieren und stören den normalen Arbeitsablauf nicht. Somit können auch Praxen und Kliniken ihren Patienten effektiven und effizienten Schutz ihrer Daten versprechen und somit auch einen wichtigen Wettbewerbsvorteil erlangen.

Mobile Security

Mobile IT-Anwendungen im Klinikum - eine Bestandsaufnahme

Wer als zukunftsorientiert gelten will, nutzt eine App. Viele Klinikanwendungen folgen diesem Trend. Kaum ein Anbieter, der auf der diesjährigen conhIT nicht eine eigene App präsentierte. Doch hält dieser Trend tatsächlich schon Einzug in den Klinikalltag?

Von Thorsten Schütz, Leiter IT/BO, Klinikum Itzehoe

Die Verbindung eines mobilen Endgerätes erfolgt typischerweise über ein WLAN. Im Homebereich mittlerweile Standard, bedeutet der Aufbau einer flächendeckenden WLAN-Infrastruktur für ein Krankenhaus eine erhebliche Investition. Oft sind dabei mehrere hundert Accesspoints nötig. Handelt es sich nicht um einen Neubau, kommen weitere Kosten für das Verlegen der zuführenden Netzwerkleitungen hinzu, bei alten Decken sind gegebenenfalls sogar Brandschutzsanierungen fällig.

Trotz dieser möglicherweise hohen Anfangsinvestition rechnet sich der Aufbau dieser Funknetzinfrastruktur meist über Projekte, die dank dieser neuen Infrastruktur überhaupt erst möglich werden: flächendeckend mobile Verfügbarkeit der Krankenhausanwendungen, VoIP-Telefonie per WLAN oder Internet per Hotspot am Patientenbett sind nur einige davon. Gerade letztgenannter Punkt wird oft vermeintlich als Nebenprodukt angesehen, ist jedoch für Patienten zunehmend ein Kriterium für die Auswahl des behandelnden Krankenhauses.

Online Ausleuchtung des Funknetzes

Eine Alternative zur Investition in eine WLAN-Infrastruktur besteht in der Abbildung des Datenverkehrs über einen Mobilfunkprovider. Die Provider sind hier in vielen Fällen bereit, in Absprache zusätzliche Mobilfunksendeantennen am Krankenhaus einzurichten, um in allen Klinikbereichen gut empfangen zu werden. Mittlerweile können innerhalb eines solchen Netzes des Mobilfunkbetreibers eigene klinikspezifische private Netzwerke abgebildet werden, die eine gesicherte Datenübertragung garantieren.

Manche Szenarien können bislang darüber jedoch noch nicht abgebildet werden, dazu gehören zum Beispiel die Ortung und die Anbindung von Medizinprodukten. Ortung im Klinikbetrieb? Was nach totalitärer Überwachung klingt, entpuppt sich bei näherer Hinsicht als ein sehr praktischer Nutzen im Alltag. Geortet werden können beispielsweise medizinische Geräte, die im ganzen Hause unterwegs sind, wie zum Beispiel rollende Ultraschallgeräte oder auch Perfusoren. Werden diese akut von einem Arzt benötigt oder befindet sich ein spezialisierter Techniker im Haus, welcher die Geräte warten soll, ist nun kein langes Suchen mehr angesagt. Mit WLAN-Tags versehene Geräte können leicht anhand der nächstgelegenen Accesspoints auf einem hinterlegten Gebäudeplan geortet werden.

Klinische Anwendungen per App

Pflegekräfte und Ärzte stehen heute oft vor einem Problem: Viele Informationen sind bereits digital verfügbar oder können direkt digital erfasst werden - nur gerade leider nicht an dem Ort, wo diese eigentlich benötigt werden oder anfallen, typischerweise direkt am Bett des Patienten. Die klassische Lösung besteht dann meist in der Verwendung eines Visitenwagens. Er kombiniert den klassischen PC mit einem Rollwagen samt Monitor und Zusatzbatterie für eine lange Akkulaufzeit.

Für die normale Visite durchaus noch praktikabel, erweist sich das Mitführen eines kompletten Rollwagens für einen kurzen Besuch beim Patienten als weitgehend unpraktisch. Ein Tablet-PC wie beispielsweise das iPad ist da leichter mitzuführen. Zudem ist die Bedienoberfläche in der Regel intuitiver bedienbar; wie eingangs erwähnt, befinden wir uns hier in einer rasanten Umbruchphase. Die Firmen stehen in der Umstellung ihrer Programme

auf eine App dabei oftmals vor der Herausforderung, ihre Entwicklerteams diesen neuen Erwartungen anzupassen.

Neben den klassischen KIS-Systemen erkennen zudem auch immer mehr sogenannte Subsystemanbieter die Vorteile einer mobilen App. PACS-Anbieter ermöglichen das mobile Betrachten von Röntgenbildern, Essenbestellungen werden per iPad noch bequemer und die digitale Patientenaufklärung unterstützt von modernen Medien wie Videos wird zunehmend real.

Medizinprodukte nutzen die Gunst der Stunde

Neben diesen klassischen Anwendungen erkennen auch die Anbieter von Medizinprodukten zunehmend das Potenzial flächendeckend bereitstehender Funknetze. Waren für Anwendungen wie Patientenmonitoring, Telemetrie oder CTG-Überwachung diese Medizintechnikgeräte bislang auf ein lokal verfügbares, zumeist proprietäres Datennetz angewiesen, setzen aktuelle Produkte zunehmend auf die vorhandene WLAN-Struktur auf.

Für das Klinikum ergeben sich daraus große Einsparpotenziale, genügt es doch nun, lediglich ein einziges Netz für alles zu betreiben - oft als One-Net-Strategie bezeichnet.

Für die IT entstehen daraus gänzliche neue Herausforderungen. Erhöhte Anforderungen an Patientensicherheit, Datenintegrität und Verfügbarkeit des Netzes bedeuten komplexe Anforderungen, nicht umsonst entwickelte sich daraus 2011 eine eigene DIN Norm.

Diese neue DIN EN 80001-1 kommt immer dann zur Anwendung, wenn das bis dato von der IT frei administrierte Datennetz mit mindestens einem Medizinprodukt gekoppelt wird. Dann gilt es plötzlich, diese neu entstandene Verbindung samt aller damit verbundenen Geräte, Netze und Programme genauestens zu dokumentieren. Zudem gilt es die Risiken zu beschreiben, die aus dieser Verbindung und den beteiligten Komponenten, aber auch den beteiligten Prozessen und Menschen, entstehen. Das ist im Übrigen keine Sache der IT oder der Medizintechnik allein - Ärzte und Pflege werden hier mit gefordert, ihr Fachwissen einzubringen. Letztlich können nur sie entscheiden, inwieweit tatsächlich ein Risiko für den Patienten entsteht und bis zu welcher Grenze dieses tolerabel ist. Daraus entstehen gänzlich neue Funktionen, wie zum Beispiel die eines Risikomanagers, und aus Sicht des Klinikbetreibers entstehen daraus ebenfalls gänzlich neue Kosten.

Neue Tools braucht das Land

Die Medizintechnik stellt also wie erwähnt eine große Herausforderung dar. Für die IT beginnt die Herausforderung bezogen auf WLAN und Mobility noch an zwei weiteren Stellen:

Zum einen erfordert die Administration eines flächendeckenden WLANs und die Beschäftigung mit der Ausbreitung und der Überwachung von Funksignalen ein spezialisiertes Wissen, um hier Verfügbarkeit und Sicherheit zu gewährleisten. Die Ansprüche an diese Verfügbarkeit steigen dabei mit jeder neuen Anwendung weiter.

Zum anderen muss die Zahl mobiler Geräte adäquat verwaltet werden. Anders als im privaten Bereich lassen sich hunderte von Tablet-PCs oder iPads nicht mehr einzeln einrichten, sondern müssen über ein Mobile Device Management (MDM) erfasst und verwaltet werden. Zahlreiche derartige MDM-Lösungen haben sich in den letzten Jahren am Markt etabliert. Diese ermöglichen die vollständige Kontrolle über das mobile Endgerät: Mit ihnen lässt sich festlegen, welche

Planung der WLAN Infrastruktur

Apps der Anwender verwenden und welche er gegebenenfalls aus einer Whitelist auswählen und zusätzlich nutzen kann. Zudem lassen sich über ein MDM abhanden gekommene Geräte lokalisieren und bei Bedarf automatisch löschen.

Fazit

So wie mobile Anwendungen im Eiltempo den privaten Bereich bereits erfolgreich durchdrungen haben, genauso zeichnet sich die rasante Ausbreitung in den klinischen Alltag von Arzt, Pflege und Funktionsbereichen ab.

Für die IT entstehen aus der Vielzahl der zu verwaltenden Endgeräte, der darunterliegenden WLAN-Infrastruktur und dem Zusammenspiel immer neuer mobiler Anwendungen - auch aus der Medizintechnik - völlig neue Anforderungen.

Für die Kliniken ergeben sich aus der Nutzung mobiler Technologien im Wettbewerb neue Chancen sowie bei geschickter Planung interessante Einsparpotenziale. ■

Wer sich über Möglichkeiten, Grenzen und Erfahrungen mit mobiler Datennutzung im Krankenhaus informieren möchte, hat auf dem Seminar ‚IT im Krankenhaus' am 23./24. September 2014 in Frankfurt die Gelegenheit dazu. Mehr Informationen unter: www.management-forum.de/it-kkh

Anwenderbericht

Verband der Ersatzkassen setzt auf Verschlüsselung von Rohde & Schwarz SIT

Sozialversicherungsdaten – beispielsweise Name, Geburtsdatum oder Familienstand – sind vom Gesetz besonders geschützt. Um die Datenübertragung zu seinem zweiten Rechenzentrumsstandort entsprechend weiter abzusichern, suchte der Verband der Ersatzkassen e.V. (vdek) in Berlin über eine bundesweite Ausschreibung eine zuverlässige IT-Sicherheitslösung. Die Entscheidung fiel schließlich auf den deutschen IT-Sicherheitsanbieter Rohde & Schwarz SIT sowie den deutschen Hersteller und Dienstleister im Bereich der Übertragungstechnologie Pan Dacom Direkt GmbH.

Von Svenja Borgschulte für Rohde & Schwarz SIT GmbH

Sozialversicherungsdaten enthalten höchst private Informationen, die nicht in unberechtigte Hände geraten dürfen. Gerade bei der elektronischen Übertragung muss jederzeit die Vertraulichkeit und Integrität zum Schutz der Daten gewährleistet sein.

Darauf legt auch der Verband der Ersatzkassen – Interessenverband und Dienstleistungsunternehmen aller Ersatzkassen in Deutschland – höchsten Wert. „Wir sehen uns in der Pflicht, stets die sichersten Verschlüsselungstechniken einzusetzen, um auch für die Zukunft einen zweifelsfreien Schutz der uns anvertrauten Daten garantieren zu können“, erklärt Peter Neuhausen, Abteilungsleiter IT des Verbandes. Der vdek trägt die Verantwortung für Dienstleistungen, die eine reibungsfreie, bundesweite Versorgung von 26 Millionen Versicherten der Ersatzkassen unterstützen.

Zur Sicherstellung der Verfügbarkeit der immer größer werdenden Datenmengen hat der vdek ein sogenanntes Remote-Backup in einem externen Datenzentrum eingerichtet. Dieses ist mehrere Kilometer von der Zentrale entfernt und über bestehende öffentliche Glasfaserverbindungen kostengünstig angebunden. Dies erfordert aber spezielle Schutzmaßnahmen: „Sensible Daten dürfen nicht unverschlüsselt über öffentlichen Grund und Boden übertragen werden“, unterstreicht der Experte des vdek. „Die Gefahr eines unauthorisierten Zugriffs wäre einfach zu hoch.“

Anforderungen: schnell, sicher, effizient

Neben dem größtmöglichen Schutz ihrer Daten sind für die Mitgliedskassen des vdek auch ein hoher Datendurchsatz und ein rasches Agieren auf sich ändernde Anforderungen wichtig. „Eine schnelle, effiziente und sichere Verschlüsselungslösung ist elementar für uns, um Massendaten in kürzester Zeit verarbeiten und bereitstellen zu können“, sagt Neuhausen.

Für die Entscheidung zwischen den Bewerbern der bundesweiten Ausschreibung waren darüber hinaus eine BSI-Zulassung, hohe Verfügbarkeit und Service entscheidend. Um ein späteres aufwendiges und teures Nachrüsten zu vermeiden, sollte die Lösung bereits jetzt eine synchrone Spiegelung der Daten ermöglichen. Entscheidende Faktoren hierfür waren eine hohe Bandbreite bei gleichzeitig geringer Latenz.

Diese Anforderungen konnte technologisch nur die SITLine ETH-Produktfamilie der Rohde & Schwarz SIT GmbH erfüllen, die die Ausschreibung zusammen mit ihrem etablierten Integrationspartner, der Pan Dacom Direkt GmbH, gewann und damit zukünftig Sozialversicherungsdaten zwischen den Rechenzentren schützt. Die Pan Dacom Direkt GmbH, einer der führenden Produktentwickler und Produktintegratoren im Bereich der Übertragungstechnik, übernimmt vom Einbau der Hardware-Lösungen über den Anschluss an die bereits bestehenden Glasfaserleitungen bis

Seit 20 Jahren leistungsstarker Partner für Gesetzliche Krankenkassen

GAI NetConsult

Sichere eHealth-Lösungen

Fokus Fachanwendungen

Online-Services
Medienbruchfreie Antragsprozesse
Behandlungsfehlermanagement
Versorgungsmanagement
Vertragsmanagement
MDK-Datenaustausch
Qualitätsmanagement Pflege
Vertriebscontrolling

Fokus Informationssicherheit

BSI- und ISO-Audits
Scan- und Penetrationstests
Aufbau von ISMS-Lösungen
Risikoanalysen
Notfallmanagement
Sichere Integrationslösungen
Architektur-Reviews
Quellcode-Analysen

Die **GAI NetConsult GmbH** ist ein bundesweit tätiges unabhängiges Software- und Consulting-Unternehmen mit besonderer Expertise in den Fachgebieten Informationssicherheit und Systementwicklung. Das Angebot umfasst dabei die qualifizierte Beratung, sowie die Konzeption und Realisierung individueller Aufgabenstellungen bis zur Einführung und Betreuung im laufenden Betrieb.

GAI NetConsult GmbH · Am Borsigturm 58 · 13507 Berlin · 030/417 898-0 · www.gai-netconsult.de

Ethernet-Verschlüsseler Rohde&Schwarz SIT SITLine ETH 40G

zur Betreuung vor Ort ebenfalls die Funktion des direkten Ansprechpartners für die systemorientierte Lösung. „Gerade für große Rechenzentren ist die Lösung von Rohde & Schwarz SIT perfekt geeignet", erklärt Yurda Oktay, Leiterin Geschäftsentwicklung der Pan Dacom Direkt GmbH. „Sie bietet höchstes technisches Niveau und ist zugleich einfach zu integrieren."

Mitlesen verhindern

Zur Absicherung der Sozialversicherungsdaten kommt konkret der Ethernet-Verschlüsseler R&S SITLine ETH40G zum Einsatz, der über das zentrale Sicherheitsmanagement SITScope einfach und intuitiv eingerichtet und administriert wird. Das SITLine ETH40G wurde speziell für den verschlüsselten Austausch riesiger Datenmengen in Echtzeit entwickelt, wie sie in Rechenzentren verwendet werden. Durch die bislang weltweit einmalige Durchsatzrate von 40 Gigabit/s bei nur 3 Mikrosekunden Latenz für die Verschlüsselung, erfüllt das neue Flaggschiff aus der SITLine ETH-Gerätefamilie die anspruchsvollen Anforderungen im Rechenzentrumseinsatz – und das bei einem Platzbedarf von nur einer Höheneinheit. Zum technischen Hintergrund: Die Verschlüsselung erfolgt bereits auf der sogenannten Sicherungsschicht (Layer2), was einen zusätzlichen Vorteil bringt: Der Security-Overhead gegenüber IP-Verschlüsselung (Layer3) ist um bis zu 40 Prozent reduziert – das spart Bandbreite. Damit ist die Geräteklasse für den vdek ideal: Sie bietet Schutz in öffentlichen Netzen ohne Abstriche bei deren Leistungsfähigkeit zu machen.

Das SITLine ETH40G setzt auf der von Rohde & Schwarz SIT eigenentwickelten Plattform-Architektur auf. Diese modulare Hard- und Software-Architektur bündelt die Vorteile von hochsicheren Individualentwicklungen und kostengünstigeren Standardlösungen für die Netzwerk-Kommunikationssicherung.

Problemlose Integration

Die Sicherung des Datenverkehrs mit Verschlüsselern der SITLine ETH-Gerätefamilie ist mit wenig Aufwand verbunden: Außer den Sicherheitsparametern sind keine weiteren netzwerkspezifischen Konfigurationen erforderlich. Sicherheitsmanagement und Netzwerkmanagement sind voneinander getrennt, sodass die SITLine ETH-Geräte problemlos in bestehende IT-Systeme integriert werden können. Dadurch entfällt eine aufwendige Anpassung der Netzwerkinfrastruktur.

SITLine ETH-Verschlüsseler sind aber nicht nur bei Punkt-zu-Punkt-Verbindungen oder Sternstrukturen einsetzbar. Durch die innovative Gruppenverschlüsselung kann auch die Übertragung in vollvermaschten „switched networks" effizient abgesichert werden. Verbände und Unternehmen können so Speicherlösungen ungefährdet auf mehrere geografisch entfernte Standorte verteilen. Dabei spielt es sicherheitstechnisch keine Rolle, ob sie zur Vernetzung gemietete oder eigene Leitungen einsetzen.

Ein weiterer Pluspunkt: Die Netzwerkverschlüsseler von Rohde & Schwarz SIT sind vom BSI für die Verarbeitung von Daten der Vertraulichkeitsgrade VS-NfD und NATO Restricted zugelassen. Gesetzliche Vorschriften zum Schutz personenbezogener Daten werden damit hundertprozentig eingehalten. „Als IT-Sicherheitspartner der Bundesregierung erfüllt Rohde & Schwarz SIT nicht nur unsere technischen Anforderungen", ergänzt Peter Neuhausen. „Wir schätzen auch die Vertrauenswürdigkeit deutscher IT-Sicherheitsprodukte."

Made in Germany

Als 100-prozentige Tochter des familiengeführten Elektronikkonzerns Rohde & Schwarz entwickelt und produziert Rohde & Schwarz SIT in Deutschland. Das hat zwei Vorteile: Zum einen ist so eine schnelle und langfristige Verfügbarkeit der Plattformkomponenten und der darauf basierenden Produkte gewährleistet. Zum anderen können sich Kunden auf die hohen deutschen Datenschutzstandards verlassen – ein wichtiger Pluspunkt, vor allem beim Einsatz von Verschlüsselungstechnik. Mit der Pan Dacom Direkt GmbH als Produktintegrator hat sich der Verband der Ersatzkassen e.V. gleichfalls für ein deutsches Unternehmen mit eigener Entwicklungsabteilung und Produktion in Deutschland entschieden. ■

Sind Sie verantwortlich für die IT-Sicherheit?
Dann lernen Sie <kes> jetzt noch besser kennen!

<kes> liefert zweimonatlich alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit, Zutrittskontrolle, Virenabwehr, Verschlüsselung, Risikomanagement, Abhör- und Manipulationsschutz, Sicherheitsplanung, Elektronische Signatur und PKI, IT-Recht, BSI-Forum

<kes> ist *die* Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

Neben den regulären Ausgaben können Sie von den <kes>-specials profitieren, die zu Messen oder besonderen Themen erscheinen.

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung Kurzmeldungen, ein Verzeichnis relevanter Veranstaltungen, außerdem aktuelle Artikel zum Probelesen und den SecuPedia Newsletter.

www.kes.info

PROBEHEFT-ANFORDERUNG

ja, bitte schicken Sie mir gratis und unverbindlich

- ☐ ein Exemplar **<kes>** - **Die Zeitschrift für Informations-Sicherheit**
- ☐ ein Exemplar **<kes> Special** „Cloud-Security“
- ☐ ein Exemplar **<kes> Special** „Mobile Security“
- ☐ ein Exemplar **<kes> Special** „Wirtschaftsspionage“

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Datum | Zeichen | Unterschrift

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Leser-Service
Postfach 12 34
55205 Ingelheim

Lieferung bitte an

Telefon Durchwahl

Mit SRC
auf der sicheren Seite

SRC ist Ihr zuverlässiger Partner beim Design, der Implementierung und dem Betrieb komplexer und sicherer Transaktions- und Informationssysteme als

- lizenzierter Auditor nach ISO 27001,
- anerkannte Prüfstelle des BSI für Common Criteria Evaluationen,
- Berater, Auditor und Gutachter für die PCI-Standards: PCI DSS, PCI PA-DSS, PCI PTS, PCI P2PE, PCI CP, PCI ASV,
- durch die BNetzA akkreditierte Prüf- und Bestätigungsstelle nach Signaturgesetz,
- anerkannter Gutachter in weiteren nationalen und internationalen Schemata (DK, gematik, DPG, GSMA, EMVCo, UKCA, APCA, MasterCard, Visa).

SRC verfügt über langjährige Erfahrungen u. a. bei

- Gutachten zur Sicherheit von Systemen und Komponenten,
- Beratung und Audits zum BSI IT-Grundschutz,
- Prüfungen nach versch. technischen Richtlinien des BSI,
- Beratung von Herstellern von Sicherheitskomponenten (z.B. SmartMeter-Gateways, Netzwerkkomponenten, Chipkarten, POS Terminals, etc.) zur Umsetzung von Anforderungen der Common Criteria,
- Erstellung von Gutachten nach den SecuRe Pay Empfehlungen der EZB,
- Unterstützung bei der Umsetzung von Vorgaben des Datenschutzes, Durchführung von Datenschutzaudits und Prüfung für die Vergabe des European Privacy Seal (EuroPriSe),
- forensischen Analysen, Quellcode-Analysen, Reverse Engineering.

Mehr unter www.src-gmbh.de

SRC
security consulting

SRC Security Research & Consulting GmbH | Graurheindorfer Straße 149a | D-53117 Bonn | Telefon: +49(0)228 2806-0 | E-Mail: info@src-gmbh.de