EHEALTHCOMPASS

IT-SICHERHEIT

IT-Sicherheit im Gesundheitswesen · Der Faktor Mensch · BSI-Kritisverordnung · IT-Sicherheit im Krankenhaus · Sicheres Entwickeln · Elektronische Siegel · Aktive Archivierung · Sicherheitsinformations- und Ereignis-Management · Cybersicherheit & Medizintechnik

EHEALTHCOM

Fordern Sie Ihr kostenloses Probeheft an und überzeugen Sie sich selbst

E-HEALTH-COM

Das unabhängige Fachmagazin für HEALTH-IT, Telemedizin und vernetzte Medizintechnik

Beate Gehm, Anzeigenleitung
Tel.: + 49 (0)69 840006 - 3030
b.gehm@health-care-com.de

oder direkt online:
www.e-health-com.eu/abo/

Spätestens seit der Cyberattacke der Schadsoftware WannCry Mitte Mai, die das britische Gesundheitswesen empfindlich getroffen hat – ein Fünftel aller englischen NHS-Trusts war betroffen – ist klar, dass IT-Sicherheit ein entscheidender Faktor bei der Vernetzung der Gesundheitsversorgung ist und die Einrichtungen entsprechend vorsorgen müssen. Mit der neuen BSI-Kritisverordnung zum Gesundheitswesen, die Ende Juni in Kraft getreten ist, wurde zumindest für größere Kliniken (mit mehr als 30 000 stationären Fällen pro Jahr) eine verbindliche Regelung seitens des Bundesamtes für Sicherheit in der Informationstechnik (BSI) getroffen. Es bleibt zu hoffen, dass die darin geforderten Maßnahmen die Entwicklung eines Branchenstandards befördern und damit die IT-Sicherheit im deutschen Gesundheitswesen flächendeckend verbessert wird. Es gibt keinen hundertprozentigen Schutz, aber es gibt zentrale Stellschrauben, an den gedreht werden kann. Die Beiträge dieses zweiten E-HEALTH-COMPASS IT-Sicherheit geben einen Überblick als auch Hinweise auf konkrete Handlungsfelder und -möglichkeiten.

Ich wünsche allen Leserinnen und Lesern eine anregende und erkenntnisreiche Lektüre.

ANNE WOLF

Projektleitung, Redaktion E-HEALTH-COM

THEMEN

04 IT-SICHERHEIT
IT-Sicherheit im Gesundheitswesen: Eine Bestandsaufnahme

10 KRANKENHAUS-IT
IT-Sicherheit im Krankenhaus

13 DER FAKTOR MENSCH
Wie kommt die IT-Sicherheit zum Menschen?

18 BSI-KRITISVERORDNUNG
Hoffen auf den Dominoeffekt

22 MEDIZINTECHNIK
Interview: Sicheres Entwickeln von Medizingeräten

FACHBEITRÄGE

26 SECRYPT
Fälschungen mit E-Siegeln von secrypt begegnen

27 TELEKOM
Einfach sicher

28 FAST LTA
Make archiving great again

29 VASGARD
Wie sicher ist mein Krankenhaus?

30 X-TENTION
Hand aufs Herz: Wie ist es um Ihr Sicherheitsniveau bestellt?

IMPRESSUM

Herausgeber: Hans-Peter Bröckerhoff | **Redaktion:** Anne Wolf (Projektleitung, v.i.S.d.P.), Silke Weidner (Korrektorat) | **Grafik:** Berta Mattern | **Anzeigen:** Beate Gehm, Tel.: +49-(0)69-840 006-3030, Mail: b.gehm@health-care-com.de | **Anschrift Redaktion und Verlag:** HEALTH-CARE-COM, GmbH Redaktion E-HEALTH-COM, Goethering 58, 63067 Offenbach | Tel.: +49-(0)69-840 006-3020, www.e-health-com.eu | redaktion@e-health-com.eu | **Druck:** Kössinger AG, Schierling | Auflage: 14 000 Exemplare; die Hälfte davon beigelegt in dem Magazin E-HEALTH-COM

© MAST3R – FOTOTLIA (UMSCHLAG)

IT-Sicherheit im Gesundheitswesen

EINE BESTANDSAUFNAHME

Nur drei Prozent aller deutschen Unternehmen sind ausreichend auf Hackerangriffe vorbereitet, zitiert die WELT [1] den TÜViT-Geschäftsführer, Dirk Kretzschmar. Wie sieht es mit der IT-Sicherheit im Gesundheitswesen aus? Welchen Bedrohungen ist die IT dort ausgesetzt? Welche Trends sind zu beobachten? Ein Überblick.

TEXT: PROF. DR. CHRISTIAN JOHNER

Bei IT-Sicherheit (englisch: IT Security) denken viele sofort an Hacker, Bot-Netze oder an Ransomware. Allerdings setzen sie damit IT-Sicherheit mit Cyber Security gleich, was nur zum Teil korrekt ist.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert IT-Sicherheit als „Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind".

Damit nennt die Definition bereits die wichtigsten Schutzziele:

- **Vertraulichkeit** der Daten (Confidentiality)
- **Integrität** der Daten (z.B. Schutz vor Verändern) (Integrity)
- **Verfügbarkeit** der Daten (Availability)

Die drei Anfangsbuchstaben der englischen Begriffe dienen als Eselsbrücke: CIA. Es gibt weitere Schutzziele wie die folgenden:

- **Zurechenbarkeit** und **Nichtabstreitbarkeit**: Wissen, wer (Personen, Rollen, Systeme) die Daten erzeugt, geändert oder gelöscht hat.
- **Authentifizierung**: Fähigkeit, den Nachweis zu führen, dass eine Person, eine Rolle oder ein System tatsächlich diejenige ist, die sie vorgibt zu sein. Dies kann unter anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen.
- **Autorisierung**: Die Fähigkeit, eine Person, eine Rolle oder ein System nur zu bestimmten Aktionen zu berechtigen.

Die Definition des Begriffs IT-Sicherheit unterscheidet aber weder, wer diese Schutzziele beeinträchtigt (z.B. innere versus äußere „Verursacher"), noch aus welchen Gründen diese beeinträchtigt werden (absichtlich versus unabsichtlich). Die Tabelle nennt Beispiele für Personen und Rollen, die die IT-Sicherheit beeinträchtigen.

Viele Definitionen des Begriffs Cyber Security zielen auf den Schutz der IT-Systeme (genauer gesagt auf die Vertraulichkeit, Integrität und Verfügbarkeit derer Daten) vor absichtlichen Angriffen von außen.

Eine weitere Begriffsdefinition stammt von der FDA, die Cyber Security auf Medizinprodukte einschränkt: „...process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient".

In beiden Fällen ist die Cybersecurity eine Untermenge der IT-Sicherheit.

IT-Sicherheit: Besonderheiten des Gesundheitswesens

Die genannten Definitionen gelten unabhängig von der Branche. Das Gesundheitswesen bzw. die Medizin weist aber einige Besonderheiten auf:

Safety und Security: Es geht um Menschenleben

Im Gegensatz zu Angriffen auf die Infrastrukturen von Privatpersonen oder Unternehmen stellen Angriffe auf IT-Infrastrukturen im Gesundheitswesen (z.B. in Kliniken) und Medizingeräte eine Bedrohung für Menschen, konkret für Patienten dar. Im Gesundheitswesen geht es meist nicht nur um Security, sondern um das höhere Ziel der Safety.

Wenn, wie geschehen, die IT einer Klinik ausfällt, kann sie keine Patienten mehr aufnehmen und muss OPs verschieben. Wenn der Angriff die Beatmungsgeräte einer Intensivstation trifft, können Patienten innerhalb von Minuten versterben.

>

Verursacher → / ↓ Motivation	INNEN	AUSSEN
ABSICHTLICH	• Frustrierte Mitarbeiter • Entlassene • Neugierige • „Spione"	• Hacker, Script Kiddies • Diebe, Hehler • (Wirtschafts-)Spione • Staatliche Stellen
UNABSICHTLICH	• IT-Admin (z.B. verschüttete Kaffeetasse) • DB-Admin (z.B. Fehler bei Wartung) • Support (falsche Konfiguration)	• Firewall-Admin (Vergessene Firewallregel) • Domain-Verwalter • KIS-Hersteller (Fehler bei Wartung) • Höhere Gewalt (Wasser, Feuer)

© MAST3R – FOTOLIA

Datenschutz und spezifische Regularien

Die Bedrohung der IT-Sicherheit im Gesundheitswesen stellt auch eine Bedrohung des Schutzes höchst vertraulicher Gesundheitsdaten dar. Auch deshalb, aber nicht nur deshalb, gibt es spezifische Regularien für die Betreiber von Gesundheitseinrichtungen und Hersteller von Medizinprodukten, die Sie weiter unten vorgestellt finden.

Manchmal führen der Datenschutz und die „Patient Safety" zu sich widersprechenden Schutzzielen: Aus Sicht des Datenschutzes und der IT-Sicherheit spricht vieles dafür, IT-Netze zu trennen und den Zugriff auf Patientendaten zu minimieren. Aus Sicht der Safety wäre es hingegen manchmal wünschenswert, wenn beispielsweise nicht nur der behandelnde Arzt die Medikationsdaten eingeben und einsehen dürfte, sondern auch die Pflegekräfte. Diese entdecken regelmäßig Fehler in Medikationsverschreibungen. Die interdisziplinäre Zusammenarbeit z.B. in onkologischen Konzilen setzt ebenfalls einen gemeinsamen Datenzugriff voraus.

Regulatorische Anforderungen

Sowohl die Klinken als auch die Hersteller müssen umfangreiche regulatorischen Anforderungen an die IT-Sicherheit erfüllen.

Die neue Medizinprodukteverordnung (MDR) fordert von den Herstellern explizit, die IT-Sicherheit zu gewährleisten und die diesbezüglichen Anforderungen an die Betreiber zu bestimmen. Auch die ISO 13485 ergänzt in ihrer aktuellen Ausgabe 2016 die Forderung, dass vertrauliche Daten geschützt werden und dass die Hersteller Anforderung an verbundene Medizinprodukte festlegen und überprüfen.

Die IEC 62304 wurde ebenfalls ergänzt: Seit dem Ammendment I (2016) fordert die Norm, dass die Software-Anforderungen – soweit angemessen – Anforderungen an die IT-Sicherheit beinhalten müssen.

Auch die FDA stellt konkrete Anforderungen, die sie in mehreren Guidance-Dokumenten zum Thema Cyber Security veröffentlicht hat. Zu den Best-Practice-Guides zählen beispielsweise der AAMI TIR/UL 2900 sowie der AAMI TIR 57.

Die regulatorischen Anforderungen betreffen ebenso die Betreiber: So gilt es, die MPBetreibV zu beachten, die den sicheren Betrieb verbundener Medizinprodukte fordert.

Das BSI-Gesetz (BSIG) wurde stark erweitert. Demnach sind Betreiber „Kritischer Infrastrukturen" (KRITIS) verpflichtet, ihre kritischen Prozesse nach dem Stand der Technik abzusichern und dies gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachzuweisen. Für Krankenhäuser liegt der Schwellenwert, ob sie als „kritisch" eingestuft werden, bei einer Fallzahl von 30 000 stationären Fällen pro Jahr.

Unabhängig von der Einstufung als KRITIS empfiehlt der Branchenarbeitskreis Medizinische Versorgung (BAK MV) u. a. ein „State-of-the-Art" Information Security Management System (ISMS) z. B. gemäß ISO 27001 und ein IT-Risikomanagement. Letzteres beschreibt die IEC 80001-1.

Weiter müssen die Betreiber den Datenschutz gewährleisten. Die IT-Sicherheit ist eine dafür notwendige, aber nicht hinreichende Voraussetzung. Eine Übersicht über weitere Standards für die IT-Sicherheit gibt der IT-Security-Navigator [2].

Lagebericht

Überblick

Bereits 38 Prozent der Unternehmen wurden laut KPMG [3] in den letzten zwei Jahren Opfer von e-Crime. In 17 Prozent der Fälle waren Gesundheitsdaten betroffen. Das BSI schreibt in seinem Lagebericht, dass täglich ca. 380 000 neue Schadprogrammvarianten gesichtet werden. „Allein bis August 2016 waren insgesamt mehr als 560 Millionen verschiedene Schadprogrammvarianten bekannt."

Leider bedrohen nicht nur „klassische Kriminelle" die IT-Sicherheit, sondern auch Angriffe [4] staatlicher Stellen bzw. von Staaten genutzte, aber nicht kommunizierte Schwachstellen wie bei der SMB-Implementierung unter Windows [5] geschehen.

Viele Kliniken agieren amateurhaft

In nur wenigen Branchen wird so wenig Geld für die IT investiert wie im Gesundheitswesen. Gemäß dem Motto „you get what you pay for" arbeitet in vielen Kliniken zu wenig und zu schlecht ausgebildetes Personal in der IT. Zudem schwächen abenteuerliche IT-Infrastrukturen und ein hohes Maß an teilweise unkoordiniertem Outsourcing an verschiedenste Akteure (z.B. Dienstleister für Drucker, Firewalls, PCs und Hotline oder Hersteller von IT-Systemen und Medizingeräten) die IT-Sicherheit.

Doch die Angriffe im Jahr 2016 haben Wirkung gezeigt. Die Krankenhäuser waren 2017 auf die Ransomware-Angriffe besser vorbereitet als im Vorjahr.

Dabei sollte aber nicht vergessen werden, dass die größte Bedrohung für die IT-Sicherheit nicht böswillige Angriffe von außen darstellen, sondern Fehler der Anwender. Systeme, die wegen vollgelaufener Festplatten ausfallen und eine ganze Kette von Krankenhäusern betreffen (wie das BSI im aktuellen Lagebericht geschildert), mögen als Beispiel dafür dienen.

Viele Hersteller handeln unverantwortlich

Die Hersteller sind für die mangelnde IT-Sicherheit mitverantwortlich. Angreifbare Infusionspumpen [6], Herzschrittmacher und klinische Informationssysteme zeugen davon. Es gibt sogar Hersteller, die IT-Schwachstellen aktiv nutzen, um Systeme remote im Krankenhausumfeld zu demonstrieren [7].

Die Ursachen für diese Probleme sind mannigfaltig:

- Viele klinische Informationssysteme und Medizinprodukte verfügen über „historisch gewachsene" Architekturen, die kaum gegen Angriffe abgeschottet werden können.
- Es herrscht oft ein mangelndes Verständnis für die Bedrohung der IT-Sicherheit, die sich durch die völlige Vernetzung von IT und Medizintechnik bei den Betreibern ergibt.
- Man beobachtet einen mangelnden Willen oder eine mangelnde Fähigkeit, während der Entwicklung und in der Post-Market-Phase die IT-Security-Risiken systematisch zu analysieren und zu beherrschen.
- Es fehlt gelegentlich die Bereitschaft, Verantwortung nicht nur für das eigene Produkt zu übernehmen, sondern für das Produkt im Kontext eines Kliniknetzes.

Trends

Die Auswirkungen mangelnder IT-Sicherheit werden in den nächsten Jahren weiter steigen. Zu diesem negativen Trend tragen auch folgende Faktoren bei:

- Die Medizinproduktehersteller >

© MAST3R – FOTOLIA

vernetzen, was vernetzbar ist. Ein integrierter Webserver zählt schon fast zum Standard. Eine Technikverliebtheit und neue Geschäftsmodelle wie „predictive maintenance“ oder „pay per use“ treiben diese Entwicklung.

- Dieser Hang zur Vernetzung macht auch vor anderen Bereichen nicht halt: Selbst Spielpuppen und Fernsehgeräte verbinden sich mit zentralen Servern. Die Glühbirne ist ebenso über Netzwerke verknüpft wie die Autos, die Heizung und natürlich die Mobiltelefone. Das Internet of Things verbindet Endpunkte, die oft nur wenige Euro kosten. Man ahnt, welche Qualität diese Produkte in Bezug zur IT-Sicherheit haben. Diese Schwachstellen bilden das (künftige) Rückgrat und das Einfallstor für großangelegte Angriffe, die nicht zwischen Unternehmen und Klinken unterscheiden.
- Die Professionalisierung der Hacker schreitet voran: Beispielsweise gehen diese arbeitsteilig vor: Die einen programmieren die Baukästen, um Bot-Netzwerke und andere Schadsoftware zu erstellen. Die Nächsten lizenzieren diese Werkzeuge und erstellen damit Schadsoftware. Die Dritten vermieten diese Netzwerke und nutzen dafür eine vierte Gruppe, die Re-Seller.
- Die Abhängigkeit von den Medizinprodukten steigt. In Bereichen wie der Molekularmedizin müssen sich die Akteure auf die (IT-) Systeme verlassen können. Einen Fehler würde man nur schwerlich bemerken, und ein Ausfall der Systeme würde diese Diagnostik und Therapie unmöglich machen. Ähnliches gilt für Closed-Loop-Systeme und selbst für die elektronische Patientenakte. Wenn es keine Akte auf Papier mehr gibt, sind die Behandelnden auf die Verfügbarkeit und Korrektheit der Daten angewiesen – und damit definitionsgemäß auf die IT-Sicherheit.

Lösungsansätze

Die Angreifer werden den Medizinprodukteherstellern und Krankenhäusern immer einen Schritt voraus sein. Wir müssen uns mit dem Gedanken anfreunden, dass es keine absolute IT-Sicherheit gibt und dass wir Tote und Verletzte als Folge mangelnder IT-Sicherheit akzeptieren müssen.

Das heißt aber nicht, dass sich die Kliniken und Hersteller einem Fatalismus hingeben dürfen. Vielmehr gilt es, die häufig überfälligen Hausaufgaben zu machen:

1. Dokumentation

Insbesondere die Klinken müssen verstehen, welche Systeme sie überhaupt haben. Das können Zehntausende Endpunkte sein, die erfasst und bewertet werden müssen. Die Dokumentation und die Übersicht sind die Voraussetzung für das Risikomanagement.

2. Risikomanagement

Die Kliniken müssen ein Risikomanagement betreiben, das hilft, die Prioritäten richtig zu setzen. Der Leitfaden des BSI [8] beschreibt Methoden zur Risikoanalyse kritischer Infrastrukturen im Gesundheitswesen.

3. IT-Sicherheit als Teil des Entwicklungsprozesses

IT-Sicherheit lässt sich nicht in Produkte „reinprüfen“. Vielmehr sollten Hersteller sie als Teil des Entwicklungsprozesses verstehen [9] und durch „Assurance Cases“ [10] bestmöglich nachweisen.

4. Konkrete Vorgaben an Betreiber

Hersteller sind gehalten, den Betreibern ganz konkrete Vorgaben zu machen und die Voraussetzungen zu beschreiben, unter denen Geräte vernetzt werden dürfen.

5. Haltbarkeitsdatum

Der Gesetzgeber müsste die Hersteller verpflichten, ein „Haltbarkeitsdatum“ festzulegen, ab dem Geräte ohne explizite Neubewertung und Beweis der IT-Sicherheit nicht mehr verwendet werden dürfen.

6. Schulung und Bewusstsein

Weil IT-Sicherheit kein ausschließlich technisches Thema ist, sondern von dem Bewusstsein und der Kompetenz der Mitarbeitenden bei Herstellern und Betreibern abhängt, ist es für die Firmen Pflicht, die Expertise systematisch zu erhöhen. Kontinuierliche Weiterbildung ist ein Muss.

7. Verantwortung des Managements

Der Fisch stinkt vom Kopf: Solange der Krankenhausdirektor glaubt, dass eine Versicherung gegen Computer-Sabotage günstiger sei als die Investition in Mitarbeitende und Infrastruktur, wird sich wenig ändern. Doch die Versicherungen reagieren: Ignoranz und Verstoß gegen Gesetze und Best Practices lassen sich kaum noch versichern.

Dass nur drei Prozent der Firmen ausreichend auf Hackerangriffe vorbereitet sind, dürfen wir im Gesundheitswesen nicht hinnehmen. Die

IT-Sicherheit ist zu einem wesentlichen Grundpfeiler einer sicheren Gesundheitsversorgung geworden. Leider, ist man versucht zu sagen: Wir könnten das Geld, das wir für IT-Sicherheit ausgeben müssen, an anderer Stelle gut gebrauchen... ■

PROF. DR. CHRISTIAN JOHNER
ist promovierter Physiker, unterrichtet an der Hochschule in Konstanz und leitet die Johner Institut GmbH.
www.johner-institut.de

REFERENZEN

1. https://www.welt.de/wirtschaft/article167165155/Deutsche-Unternehmen-eine-leichte-Beute-fuer-Hacker.html
2. https://www.security-standards.de/ITSecurityGrid.html
3. http://hub.kpmg.de/hubfs/LandingPages-PDF/e-crime-studie-2017-KPMG.pdf
4. http://www.theregister.co.uk/2015/02/17/kaspersky_labs_equation_group/
5. https://arstechnica.com/information-technology/2017/04/nsa-backdoor-detected-on-55000-windows-boxes-can-now-be-remotely-removed/
6. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm
7. https://arstechnica.com/information-technology/2017/04/security-vendor-uses-hospitals-network-for-unauthorized-sales-demos/
8. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/RisikoanalyseKrankenhausIT_Leitfaden_pdf.html
9. http://2.bp.blogspot.com/-7Hr15ZJhi34/VnPYDOlTxtI/AAAAAAAAETQ/hU7uJxEQEik/s640/600px-Security_in_the_SDLC_Process.png
10. http://slideplayer.com/slide/678947/1/images/32/Security-specific+example+of+an+assurance+case+(moderate+threat).jpg

ANZEIGE

Wie sicher ist mein Krankenhaus?

Vernetzte Medizintechnik – komfortabel und effizient, aber auch überaus einladend für Angreifer. Wie Sie Ihr Netzwerk zuverlässig und ressourcenfreundlich schützen, erklärt Geschäftsführer Michael Pöhlsen in dieser Ausgabe des Compass IT-Sicherheit.

Holistic Cyber Intelligence
Kostenloses White Paper: www.vasgard.com/pki

VASGARD

IT-Sicherheit
IM KRANKENHAUS

Chinesen haben ein Sprichwort für die Situationsbeschreibung der Sicherheit von informationstechnischen Systemen in Kliniken: „Jedes Ding hat drei Seiten. Eine, die ich nicht sehe, eine, die Du nicht siehst und eine, die wir beide nicht sehen."

TEXT: MICHAEL THOSS

Wie sollen wir das verstehen? Die eine Seite ist der rein technische Umgang mit potenziellen Angriffen. Die Aus- und Aufrüstung von Firewalls, Virenscannern, Malware-Detection- und Intrusion-Detection-Systemen als ein Beispiel. Das ist die einfach zu sehende Seite, bei der man darauf hofft, dass Technologie Probleme löst. Was allgemein und bei Cybersicherheit nicht funktionieren kann, aber zumindest die Ausgangsposition verbessert. Technologie alleine hat noch nie irgendein Problem gelöst. Nur weil wir Daten sichern, heißt das ja noch lange nicht, dass wir mit der Sicherung auch etwas anfangen können – wenn wir sie brauchen.

Was uns zur zweiten Seite bringt: Sicherheit ist und war in erster Linie immer eine Frage des Bewusstseins. Des Bewusstseins auf jeder Unternehmensebene. Von der niedrigsten bis zur höchsten. Für alle gelten die gleichen Gefährdungsrisiken und folglich Regelungen. Häufig ist exakt dieser Umstand ein erhebliches Manko von Sicherheitsarchitekturen. Während die IT des Krankenhauses sich bemüht, das Krankenhausinformationssystem zu schützen (in seiner Gesamtheit), ist da immer das eine Medizintechniksystem, das trotz aller Sicherheitsbedenken unbedingt eingebunden werden muss. Oder das Mail-System, das zwar der normale Mitarbeiter nicht unbedingt benötigt, die Geschäftsführung aber auf jeden Fall... Obwohl gerade für Letzteres diverse Alternativen ständig zur Verfügung stehen. Vielleicht erinnern sich manche, von „digitaler Sorglosigkeit“ geprägte Mitarbeiter des Unternehmens nicht mehr, dass man mittels Fax ebenfalls Texte versenden kann und anstatt WhatsApp ruhig mal das Telefon bemühen könnte. Zumindest wenn gerade eine Krise herrscht.

Bleibt die dritte Seite: Hundertprozentige Sicherheit ist in der Informationstechnik nicht möglich. Das weiß jeder, aber keiner will es wahrhaben („sehen“). Das bedeutet, dass im Falle eines Risikoeintritts wie zum Beispiel im Falle einer Cyberattacke nur eine Instanz des Unternehmens Entscheidungen treffen darf: Die IT. Diese ist wiederum durch ihre verantwortlichen Leitungsfunktionen (am Ende immer die Geschäftsführung) zu befähigen, die erforderlichen Schritte umzusetzen.

Im Idealfall vor dem Risikoeintritt. Wenn ein Risiko eingetreten ist, befinden wir uns bereits in der Krise und folglich im Krisenmanagement. Wichtig ist, dass es sich nicht um das Gleiche handelt. Eine Krise ist ein eingetretenes Risiko und erfordert andere Mittel als die zuvor in die Vermeidung oder Verminderung eines Risikos investierten Mittel.

Zu den zu investierenden Mitteln zählt vor allem die Sensibilisierung der Mitarbeiter des Unternehmens für die Risiken. Im Falle der Integration von medizintechnischen Systemen können wir die DIN 80001 umsetzen. Im Falle einer nichtkritischen Infrastruktur (nach ITSiG) können wir trotzdem einen IT-Sicherheitsbeauftragten qualifizieren und mit den erforderlichen Kompetenzen ausstatten. Wir können freiwillig am UP KRITIS teilnehmen und wir können freiwillig die Budgets der IT für den Sicherheitsbereich – was auch Personal bedeuten kann – dem Zeitgeschehen anpassen.

Krankenhäuser sind heute vermutlich gefährdeter als noch vor einigen Jahren, aber nicht weil sie zu wenig tun, sondern weil sie in der „Digitalen Öffentlichkeit“ schlichtweg heute viel präsenter sind. Vor allem das Internet der Dinge (das bedeutet im engeren Sinne immer „Fernwartung“ oder „Fernzugriff“) schafft ständig neue Sicherheitslücken in virtuellen Systemen, deren ältere Bestandteile (wie Medizintechnik) oftmals nicht aktueller Stand der Technik sind. Die Veränderungszyklen der Informationstechnik sind schlichtweg viel schneller als Zyklen anderer Technologiebereiche und die verschiedenen Welten müssen sowohl technisch als auch organisatorisch schneller angeglichen werden.

Im Juli 2017 veröffentlichte der BAK (Branchenarbeitskreis) Medizinische Versorgung im Rahmen der UP KRITIS (Umsetzungsplan Kritische Infrastruktur) seine Handlungsempfehlungen zur Verbesse >

© NICESCENE – FOTOLIA

rung der Informationssicherheit an Kliniken. Das Dokument umfasst 15 Seiten, darin elf Seiten mit Hinweisen, Prüffragen und Empfehlungen. Das komplette Dokument ist frei verfügbar und kann im Internet u.a. über die Website des Bundesverbands der Krankenhaus-IT-Leiterinnen/Leiter e.V. www.kh-it.de als Download bezogen werden.

Wichtige Hinweise finden sich im Management Summary. So läuft mit Veröffentlichung der BSI-KritisV die zweijährige Übergangsfrist zur Erreichung der Ziele. Im Anschluss drohen den Pflichtteilnehmern mit über 30 000 stationären Fällen pro Jahr Bußgelder. Die Maßnahmen erfordern einigen Aufwand von den aktuell betroffenen circa 110 Krankenhäusern (Trägern). Man darf vermutlich auch annehmen, dass bei noch knapp 2 000 Krankenhausstandorten in Deutschland über kurz oder lang die Frage aufkommen wird, ob diese 110 Einheiten ausreichen. Bedenkt man die Bundesländer mit niedrigen Einwohnerzahlen und ländliche Regionen, so könnte das Thema Sicherheit der Versorgung durchaus auf andere Kliniken erweitert werden.

Besonders bemerkenswert in den Empfehlungen des BAK Medizinische Versorgung sind mehrere Punkte. Zum einen ist da die Fokussierung auf das leitende Management der Kliniken. Ohne dessen maßgebliche Unterstützung sind die vorgegebenen Ziele nicht erreichbar. Zum anderen weist der BAK mehrfach und ausdrücklich darauf hin, dass es sich bei der Informationssicherheit nicht um ein auf die IT beschränktes Thema handelt. Medizintechnik, Haustechnik, Kommunikationstechnik und weitere Aspekte sind unter den gleichen Rahmenbedingungen zu handhaben. Das vervielfacht den Aufwand und ist in den meisten Einheiten nicht mit vorhandenem Budget und Personal zu bedienen. Dieser Schluss wird durch den BAK explizit bestätigt. Durch die Einbeziehung der sonstigen Technologiebereiche, die alle als Nutzer von IT-Infrastruktur auftreten, wird zudem das schwer greifbare Thema des Internet der Dinge Bestandteil der Sicherheitsmaßnahmen.

»Das Internet der Dinge schafft ständig neue Sicherheitslücken in virtuellen Systemen.«

Erfreulich ist zudem, dass der BAK explizit eine Intensivierung bzw. konsequente Umsetzung der unternehmensinternen Schulungen zum Thema IT-Sicherheit fordert. Die Ermittlungsbehörden der Länder sehen schon lange in der oftmals herrschenden „digitalen Sorglosigkeit“ der IT-Nutzer ein großes Problem im Rahmen der Informationssicherheit. Darüber hinaus hat der BAK ausdrücklich festgestellt, dass IT-Notfallpläne nicht ausreichen, um eine entsprechende Krise zu bewältigen. Dafür sind nicht-IT-gestützte Ausfallverfahren, sogenannte Papierersatzverfahren, vorzuhalten. Was an dieser Stelle vielleicht fehlt, ist die Feststellung, dass es nicht Aufgabe der IT ist, diese Notfallverfahren zu definieren. Es ist Aufgabe der Fachabteilungen im Rahmen ihrer Verantwortung für Patienten und Prozesse.

Die Handlungsempfehlungen liefern dem interessierten Leser zudem eine Übersicht über weitere relevante oder nutzbare Dokumente. Die Lektüre ist für Management und IT-Verantwortliche dringend zu empfehlen.

Eines sollten wir bei alldem nicht vergessen: Es werden in Deutschland nicht „speziell“ Krankenhäuser angegriffen. Vermutlich waren es sogar fast ausschließlich „Kollateralschäden“ von breit angelegten (vielleicht auch nur testweisen) Angriffen, die ebenso Industrie, Geldinstitute, Behörden und andere Gruppen trafen. Auf einen Warnschuss sollte man jedoch immer angemessen reagieren. Im Falle der BSI-KritisV empfiehlt sich die Auseinandersetzung auch für Häuser unter 30 000 stationären Fällen. Niemand weiß, was die Zukunft bringt, deswegen sind Prognosen auch so schwierig. Jeder Verantwortliche sollte bedenken, dass die ausgesprochenen Handlungsempfehlungen einen rechtlichen Hintergrund haben und daher nicht ignoriert werden können. ■

MICHAEL THOSS

ist Mitglied im Bundesverband KH-IT, Autor und Berater (StrukturtrifftFraktal – IT-Kompetenz und Beratung für Kliniken).

Wie kommt die IT-Sicherheit ZUM MENSCHEN?

Der „Faktor Mensch“ rückt zunehmend in den Fokus des Interesses, wenn es um IT-Sicherheit geht. Doch wie schafft man bei den Nutzern ein Bewusstsein für sichere und unsichere Verhaltensweisen? Und wie veranlasst man sie, ihr Verhalten zu ändern? Eine Lösung bietet „The Analogies Project“ mit einem Storytelling-Ansatz. Doch auch die Etablierung einer Fehlerkultur im Gesundheitswesen wäre ein wichtiger Beitrag.

© ALEUTIE – FOTOLIA

TEXT: CHRISTINA CZESCHIK

>

Wenn man Fachkongresse und Veröffentlichungen in der Informationssicherheit in den letzten Monaten verfolgt, fällt auf: Neben dem herkömmlichen technischen Wettrüsten zwischen Verteidigern und Angreifern rückt immer mehr der sogenannte „Faktor Mensch“ in den Fokus des Interesses. Keinen Moment zu früh, denn obwohl Social Engineering schon mehrere Tausend Jahre älter ist als das Internet, ist der Mensch auch in modernen IT-Systemen für Angreifer oft der verletzlichste Eintrittspunkt in ein System. So war im Jahr 2016 bei etwa 70 Prozent der erfolgreichen (festgestellten) Attacken Social Engineering ein wichtiger Teil der Angriffsstrategie – und nur bei etwa zwei Prozent der Angriffe kam ein Zero Day Exploit zum Tragen, also eine neu entdeckte technische Sicherheitslücke [1].

Die zentralen Fragen, die jene bewegen, die an der Schnittstelle zwischen IT-Sicherheit und Mensch sitzen, lauten: Wie schafft man bei den Nutzern ein Bewusstsein – neudeutsch Awareness – für sichere und unsichere Verhaltensweisen? Und wie veranlasst man sie, aus diesem Bewusstsein heraus ihr Verhalten zu ändern?

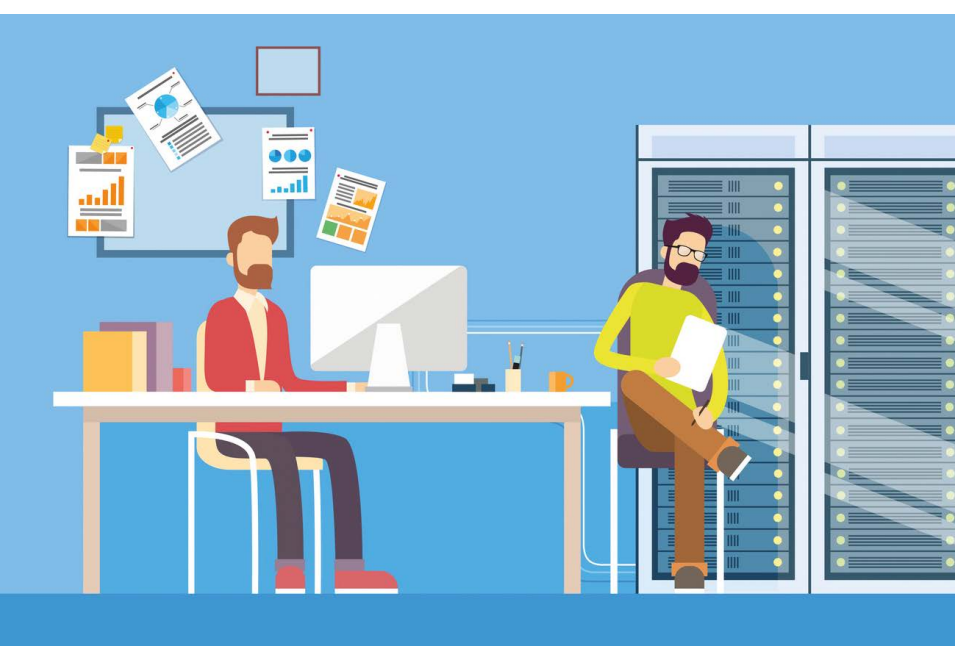
Anleihen aus der Werbepsychologie: AIDA

Eine effektive Aufklärung und die Motivation zur Verhaltensänderung sind auch in anderen Bereichen als der Informationssicherheit gefragt, etwa in der Werbepsychologie. Dort wird dieser Prozess unter dem Akronym „AIDA“ zusammengefasst:

- Attention – Aufmerksamkeit beim Kunden erzeugen
- Interest – das Interesse des Kunden wecken
- Desire – das Bedürfnis nach dem Produkt wecken
- Action – den Kunden zum Kauf bewegen

Diese Ziele der Werbepsychologie lassen sich fast eins zu eins auf die Sensibilisierung in der Informationssicherheit übertragen – es bietet sich lediglich an, nach dem Wecken des Bedürfnisses einen weiteren Schritt einzuschieben, um der oft komplexen Materie gerecht zu werden:

- Attention – Aufmerksamkeit beim Nutzer erzeugen
- Interest – Interesse für das Thema Informationssicherheit wecken
- Desire – beim Benutzer das Bedürfnis nach Informationssicherheit wecken
- Information – den Nutzer schulen
- Action – den Nutzer zur Verhaltensänderung bewegen



Im Fokus: Der unmittelbare Nutzen

Schon die ersten beiden Schritte dieses „AIDIA“-Prozesses erweisen sich als schwierig: Benutzer in einem IT-System sind in der Regel darauf fokussiert, ihre anstehenden Aufgaben zu erledigen – also alles, was ihnen unmittelbaren Nutzen bringt. Dies kann die zeitige Erledigung ihrer täglichen To-do-Liste sein, um pünktlich Feierabend machen zu können, oder auch die Lustgewinn versprechenden Aktivitäten auf Facebook oder Twitter in (oder außerhalb) der Mittagspause. Im Empfinden der meisten Nutzer trägt die Informationssicherheit an keiner Stelle zur Zielerreichung bei. Ohne

© MAST3R – FOTOLIA

Aufmerksamkeit und Interesse lässt sich kein Bedürfnis nach Informationssicherheit wecken, und auch die besten Informationsressourcen und Schulungsprogramme stoßen schließlich auf taube Ohren; das Nutzerverhalten ändert sich nicht.

Kurz gesagt: Die Informationssicherheit wird vom Nutzer als irrelevant empfunden. Bei vielen Nutzern, bei denen es anfänglich gelingt, sie für Sicherheitsfragen zu sensibilisieren, tritt dann ein zweites Problem hinzu: Die IT wird als „Black Box" wahrgenommen und Gefahren, die aus dem Netz drohen, als unbeherrschbar und schicksalhaft.

The Analogies Project: Storytelling als Methode

Was tun? Eine Lösung: Das Geschichtenerzählen (Storytelling) als älteste und bewährteste Form der Fortbildung und des Wissenstransfers, die den Menschen zur Verfügung steht. Wie der US-amerikanische Literaturwissenschaftler Jonathan Gottschall in seinem Buch „The Storytelling Animal" [2] darlegt, hat sich der menschliche Intellekt parallel zum und gemeinsam mit dem Geschichtenerzählen entwickelt: Solche Geschichten, die von Menschen als spannend wahrgenommen werden, sind für den Transport wichtiger Informationen optimiert, und der menschliche Geist hat sich entsprechend so entwickelt, dass spannende, gehaltvolle Geschichten seine Aufmerksamkeit unweigerlich auf sich ziehen.

Diese Erfahrung hat auch der britische Sicherheitsberater Bruce Hallas in seiner Berufspraxis gemacht. Mit einem Ausbildungshintergrund in Jura und Marketing hat ihn nach Gründung seiner Beratungsfirma Marmalade Box lange die Frage umgetrieben, wie man die Informationssicherheit für IT-Laien attraktiv gestalten könnte. Eines der Ergebnisse ist The Analogies Project, ein von ihm ins Leben gerufenes Webportal [3]. Hier werden Analogien aus der IT-Sicherheit gesammelt, die erdacht und teilweise aus anderen Sprachen übersetzt wurden – von Mitwirkenden aus mittlerweile zehn Ländern. Die Beiträge erläutern unter anderem, warum ein Datenschutzbeauftragter im Unternehmen manchmal vorgehen muss wie professionelle Aufräumer in Messie-Haushalten im Privatfernsehen [4], warum Informationssicherheit mit Sonnenschutz zu vergleichen ist [5] (nicht nur auf die offensichtlichste Art und Weise) und wie der Löwe der Informationssicherheit zu seinen Zähnen kommt [6]. Ein walisischer Komiker berichtet davon, wie einst seine Identität gestohlen wurde [7], und eine Rumänin vergleicht die Informationssicherheit mit einem Land, das den meisten Laien so fremd ist wie einem Briten Rumänien [8].

Schon in den 2000er-Jahren wurde im amerikanischen Militär das Storytelling als Methode eingesetzt, um die Sensibilität der Soldaten für Sicherheitsfragen (nicht nur, aber auch im Cyberspace) zu verbessern. Dabei wurden von Dr. Dee H. Andrews vom U.S. Air Force Research Laboratory die folgenden vier Formen von Geschichten identifiziert, die in Fortbildungen und Awareness-Kampagnen effektiv sein können [9]:

- Erzählungen
- Fallstudien
- Szenarien
- Problembasiertes Lernen

Die Reihenfolge der Aufzählung entspricht einer zunehmenden aktiven Einbeziehung des Lernenden: So richten sich Erzählungen an intellektuell weitgehend passive Zuhörer, bewirken jedoch im besten Fall eine emotionale Mitbeteiligung, die eine wichtige Rolle bei Awareness und Sensibilisierung auch in der Informationssicherheit spielt. Paradebeispiele wären hier etwa Unterhaltungsfilme, die Themen aus der Informationssicherheit emotional aufbereiten, wie etwa „Snowden" des Regisseurs Oliver Stone.

Fallstudien und Szenarien beinhalten Situationen, die sich in der Vergangenheit entweder so zugetragen haben oder sich zumindest so hätten zutragen können – also authentisch sind. Das Szenario, im Gegensatz zur Fallstudie, hat dabei keinen festgelegten Ausgang: Verschiedene Handlungsoptionen und ihre möglichen Konsequenzen werden von den Teilnehmern diskutiert, ohne dass der „Erzähler" – also in diesem Fall der Veranstaltungsleiter – als letzte Instanz eine Auflösung liefert. So könnte beispielsweise in deutschen Krankenhäusern die weithin bekannt gewordene Ransomware-Attacke auf das Lukaskrankenhaus in Neuss Stoff für eine Fallstudie oder die Bearbeitung eines Szenarios liefern.

Noch ergebnisoffener ist das problembasierte (oder problemorientierte) Lernen. Hier verzichtet die Moderatorin weitgehend darauf, die Lösungswege der Teilnehmer zu bewerten. Im Vordergrund steht vielmehr das Training des Treffens von Entscheidungen aufgrund unvollständiger Informationen – in der realen Welt eher die Regel als die Ausnahme.

>

Interesse, Aufmerksamkeit und Bedürfnis wecken

Um zum „AIDIA"-Modell vom Anfang zurückzukommen: Wo setzt das Geschichtenerzählen hier an, um das Ziel „Action" zu erreichen? Zunächst ganz am Anfang, bei der Aufmerksamkeit: Kognitiven Wissenschaftlern zufolge lenken Geschichten sehr effektiv die Aufmerksamkeit auf die Punkte eines Sachverhalts, die wichtig sind und im Gedächtnis haften bleiben sollen – also den Hauptstrang der Handlung. Nebensächlichkeiten werden auch als solche erkennbar und spielen höchstens eine Rolle, um die Spannung im Hauptstrang der Handlung zu erhöhen.

Interesse und der Wunsch (Desire) nach einer Handlungsänderung werden durch zwei weitere Charakteristika der Geschichte geweckt. Die erste davon ist Selbstbezug: Der Zuhörer oder Leser versetzt sich unweigerlich in die Rolle des Protagonisten – sei es nun Edward Snowden im Film oder der IT-Leiter des Lukaskrankenhauses in einer Fallstudie – und beantwortet damit die bei neuen Lerninhalten stets mitschwingende Frage: „Wozu brauche ich das?". Zweitens aktiviert die Geschichte Emotionen und weckt somit auf direktestem Weg Bedürfnisse, etwa, eine als gefährlich wahrgenommene Situation zu verhindern.

Die emotionale Komponente trägt auch zur besseren Abspeicherung von Information bei. Verantwortlich ist hier die Amygdala, ein Kerngebiet des Gehirns, das sowohl für emotionale Verarbeitung als auch das Anlegen von Gedächtnisinhalten verantwortlich ist. Optimal ist für die Abspeicherung im Gedächtnis eine mittelstarke emotionale Aktivierung; bei geringer Aktivierung herrscht Desinteresse und es findet kein Lernen statt, bei äußerst starker Aktivierung sind Gedächtnisinhalte später möglicherweise nicht mehr abrufbar. Hier kommt ein weiterer Vorteil der Geschichte ins Spiel: Durch den reichen Kontext innerhalb einer Geschichte wird die Wissensorganisation verbessert. Einzelne Fakten werden mit einer Vielzahl anderer verknüpft, was den späteren Abruf erleichtert.

Um es noch einmal mit „AIDIA" zusammenzufassen: Mithilfe einer Geschichte wird Aufmerksamkeit und Interesse erzeugt, es kann ein Bedürfnis (Desire) nach Informationssicherheit geschaffen werden und es werden in leicht zu merkender Form Informationen darüber transportiert, wie Informationssicherheit zu erreichen ist.

Zum Schluss: Action!

Hier fehlt – Sie haben es gemerkt – der letzte Teil, die „Action": Das Schaffen von Awareness ist zwar ein wichtiger und notwendiger Schritt auf dem Weg zur Verhaltensänderung, ist aber allein nicht genug, um Menschen dazu zu bewegen, alte Gewohnheiten abzulegen. Um noch einmal zum Anfang zurückzukommen: Nicht nur die Werbepsychologie, sondern auch die Medizin und das Gesundheitswesen beschäftigt seit Jahrzehnten die Frage, wie man das Verhalten eines Menschen nachhaltig ändern kann. Hier wurde das transtheoretische Modell (TTM) entworfen, das den Weg des Menschen vom Desinteresse zur Handlung ebenfalls in Stadien einteilt [10]:

- Absichtslosigkeit,
- Absichtsbildung,
- Vorbereitung
- Handlung und
- Aufrechterhaltung.

Wie gut die Aussichten eines Individuums sind, vom Stadium der Absichtslosigkeit zu den Stadien der Handlung und Aufrechterhaltung fortzuschreiten, hängt ganz wesentlich von seiner Selbstwirksamkeit ab – der Zuversicht, die eigenen Handlungen und deren Ergebnis beeinflussen zu können. Storytelling fördert insbesondere dann die Selbstwirksamkeit von Probanden, wenn diese selbst die Erzählenden sind [11] – dies zeigt, dass der Einsatz von „Frontal"-Storytelling nur die halbe Miete sein kann, wenn es darum geht, Awareness und Verhaltensänderung zu erzielen. Ebenso wichtig ist es, Nutzern unabhängig von Kenntnisstand und Fähigkeiten die Möglichkeit zu geben, ihre Erfahrungen im Umgang mit IT und Informationssicherheit auszutauschen, ohne negative Konsequenzen befürchten zu müssen – eben ihre eigenen Geschichten zu erzählen, auch und gerade wenn diese Geschichten von Fehlern und unnötig eingegangenen Risiken handeln. Anders gesagt: Die lange überfällige Fehlerkultur im Gesundheitswesen, die in den letzten Jahren langsam etabliert wurde, muss auch die Informationssicherheit einschließen. ■

DR. MED. CHRISTINA CZESCHIK
ist Ärztin für Medizinische Informatik und Fachautorin für eHealth und Informationssicherheit.

REFERENZEN

Mehr Informationen zu Storytelling in der Informationssicherheit: ***www.serapion.de/story***

1. Verizon: Human error still among the top data security threats [Internet]. SearchCompliance. [zitiert 29. Juli 2017]. Verfügbar unter: http://searchcompliance.techtarget.com/feature/Verizon-Human-error-still-among-the-top-data-security-threats

2. Gottschall J. The storytelling animal: how stories make us human. Boston: Houghton Mifflin Harcourt; 2012. 248 S.

3. The Analogies Project – Finding The Hidden InfoSec Story [Internet]. The Analogies Project. [zitiert 30. Juli 2017]. Verfügbar unter: https://theanalogiesproject.org/

4. Data Hoarders [Internet]. The Analogies Project. [zitiert 30. Juli 2017]. Verfügbar unter: https://theanalogiesproject.org/the-analogies/data-hoarders/

5. Infosec is Like Sun Protection [Internet]. The Analogies Project. [zitiert 30. Juli 2017]. Verfügbar unter: https://theanalogiesproject.org/the-analogies/infosec-like-sun-protection/

6. Security with Teeth [Internet]. The Analogies Project. [zitiert 30. Juli 2017]. Verfügbar unter: https://theanalogiesproject.org/the-analogies/security-with-teeth/

7. Don't Pin Me Down [Internet]. The Analogies Project. [zitiert 30. Juli 2017]. Verfügbar unter: https://theanalogiesproject.org/the-analogies/dont-pin-2/

8. Infosec? What country is that? [Internet]. The Analogies Project. [zitiert 30. Juli 2017]. Verfügbar unter: https://theanalogiesproject.org/the-analogies/infosec-country/

9. Andrews DH, Hull T, DeMeester K. Storytelling as an instructional method: research perspectives. Rotterdam; Boston: Sense Publishers; 2010.

10. Prochaska JO, Velicer WF. The transtheoretical model of health behavior change. Am J Health Promot AJHP. Oktober 1997;12(1):38–48.

11. Li L. Digital Storytelling: Self-Efficacy and Digital Literacy. In Association for the Advancement of Computing in Education (AACE); 2006 [zitiert 3. August 2017]. S. 2159–64. Verfügbar unter: https://www.learntechlib.org/p/24031/

FAST LTA
Wir sichern Petabytes.

Silent Bricks:

Mit linearer, struktur-sicherer Speicherung gegen Datenverlust gewappnet.

2016 war das Jahr der **Ransomware**. Noch nie gab es so viele Angriffe, noch nie waren so viele Unternehmen betroffen, noch nie wurde so viel „Lösegeld" bezahlt. Schutz bieten nur Speichersysteme, die Daten aus Backups und Archiv manipulationssicher speichern.

http://bit.ly/ransomware-info

FAST LTA AG | Email: info@fast-lta.de | **www.fast-lta.de**

Hoffen auf den DOMINOEFFEKT

Seit dem 30. Juni 2017 ist der zweite Korb der BSI-Kritisverordnung zur IT-Sicherheit kritischer Infrastrukturen in Kraft. Entscheidend wird sein, ob es gelingt, den zu entwickelnden Standard auch in die kleineren Häuser zu tragen, die von der Verordnung primär nicht betroffen sind.

TEXT: PHILIPP GRÄTZEL VON GRÄTZ

Auf den ersten Blick scheint das Thema der IT-Sicherheit in kritischen Infrastrukturen relativ klar umrissen. Die Bundesregierung will kritische Infrastrukturen besser vor IT-Angriffen schützen. Das ist seit dem IT-Sicherheitsgesetz aus dem Jahr 2015 gesetzt. Für das Gesundheitswesen hat jetzt die am 30. Juni 2017 offiziell in Kraft getretene BSI-Kritisverordnung die nötigen Konkretisierungen gebracht, sodass die eigentliche Arbeit in den medizinischen Einrichtungen beginnen kann.

Angesprochen sind demnach Krankenhäuser mit mehr als 30 000 stationären Fällen pro Jahr, was je nach Rechnung 110 bis 120 Einrichtungen deutschlandweit betrifft. Diese Einrichtungen müssen innerhalb der gesetzlichen Frist von sechs Monaten, also bis zum 30. Dezember 2017, eine Kontaktstelle benennen, die rund um die Uhr für das BSI ansprechbar ist. Sie ist ab Benennung verpflichtet, „erhebliche" Störungen dem BSI zu melden. Das BSI wiederum informiert die Kontaktstellen zeitnah über sicherheitsrelevante Entwicklungen. Die Kommunikation läuft also in zwei Richtungen.

Eine weitere Frist ist der 30. Juni 2019, also zwei Jahre nach Inkrafttreten der Verordnung. Bis dahin müssen Einrichtungen, die die kritische Größe erreichen, nachweisen, dass sie IT-Sicherheitsmaßnahmen „nach dem Stand der Technik" umgesetzt haben. So weit, so klar. Dass es trotz dieser relativ eindeutigen Rahmenbedingungen noch erheblichen Diskussionsbedarf gibt, machte eine von RS Medical Consult organisierte und konzipierte Veranstaltung zur IT-Sicherheit in Berlin deutlich, die einen Tag vor der Veröffentlichung der BSI-Kritisverordnung im Bundesgesetzblatt stattfand.

Warten auf den Branchenstandard

Drei Themenbereiche brennen den Krankenhäusern besonders auf den Nägeln. Da ist zum einen die Frage, was die Anforderungen der BSI-Kritisverordnung ganz konkret bedeuten. Die zweite Frage ist die nach der Finanzierung. Und der dritte Themenkomplex dreht sich darum, wie die innenpolitische Anforderung nach mehr Sicherheit einerseits und die gesundheits- und forschungspolitische Anforderung nach mehr Offenheit – Stichwort einrichtungsübergreifende, intersektorale und durch Big-Data-Anwendungen optimierte Versorgung – andererseits unter einen Hut zu bringen sind. Eng verbunden mit dieser letztgenannten Problematik ist der Umgang mit jenen Einrichtungen, die nicht unter die BSI-Kritisverordnung fallen, weil sie formal zu wenige stationäre Fälle haben.

Was die konkreten Anforderungen an den Stand der Technik angeht, den KRITIS-Häuser bis Ende Juni 2019 umzusetzen haben, liegt das Augenmerk derzeit auf dem im Rahmen des KRITIS-Prozesses etablierten Branchenarbeitskreis Gesundheit. Ziel des IT-Sicherheitsgesetzes sei es nie gewesen, dass der Gesetzgeber bis ins kleinste Detail durchreguliere, welche Maßnahmen zu treffen seien, betonte Matthias Fischer, im Bundesinnenministerium zuständiger Referent für KRITIS: „Die Unternehmen sind vielmehr aufgefordert, sich an einen Tisch zu setzen und branchenspezifische Sicherheitsstandards zu entwickeln."

Es würde sich zudem anbieten, im Rahmen dieses Prozesses auch gleich Regelungen zur Zertifizierung zu formulieren, so Fischer. Denn das ist eine weitere Anforderung von KRITIS: Alle zwei Jahre müssen die „kritischen" Einrichtungen eine Zertifizierung durchlaufen. Die könnte sich zu einem veritablen Flaschenhals auswachsen, weil entsprechend qualifizierte Experten derzeit auf dem Markt kaum zu bekommen sind. IT-Sicherheitsexperten werden im Moment quasi von den Universitäten weggekauft. Und weil sie so gefragt sind, können sie sich oft die gut zahlenden Arbeitgeber aussuchen, die eher nicht im Gesundheitswesen zu finden sind.

Jan Neuhaus, für IT zuständiger Geschäftsführer der Deutschen Krankenhausgesellschaft (DKG), regte in Berlin an, über eine Art „Ring-Auditierung" der Krankenhäuser untereinander nachzudenken. Die BSI-Kritisverordnung gäbe das durchaus her, denn auch bei der Auditierung/Zertifizierung werden die Details den jeweiligen Branchen überlassen. Entsprechende Non-Disclosure-Agreements vorausgesetzt, hätte eine wechselseitige Auditierung der Krankenhäuser unter anderem den Vorteil, dass gesundheitssysteminterne IT-Sicherheitsexpertise aktiv aufgebaut würde. Es gäbe also neben der Auditierung auch eine Art Fortbildungskomponente.

Auch sinnlose Investitionen schaden Patienten

Wie auch immer die Details am Ende aussehen, der branchenspezifische Sicherheitsstandard, im KRITIS-Slang B3S abgekürzt, müsse für das Gesundheitswesen bis Ende des Jahres fertig sein, wenn die gesetzlichen Fristen gehalten werden sol- >

© PSDESIGN1 – FOTOLIA

len, so Neuhaus. Angesichts des mittlerweile in Gang gekommenen Dialogs zwischen Krankenhäusern und den beiden Bundesministerien des Inneren und der Gesundheit äußerte er sich optimistisch, dass dies auch gelinge.

Definitiv nicht angebracht sei Panikmache, so der DKG-Geschäftsführer: „Für kleinere Häuser ist diese Panikmache zum Teil unlustig. Es rennen derzeit Versicherungen herum, die abstruse Policen anbieten. Es rennen Berater herum, die Honorare wollen, ohne eine spezielle Qualifikation zu haben. Panik ist kein guter Ratgeber für Entscheidungen in lebenskritischen Situationen. Auch Investitionen in unschädliche, aber nutzlose Produkte oder Dienstleistungen schaden indirekt den Patienten."

Schon bevor der branchenspezifische Sicherheitsstandard vorliege, sollten von KRITIS betroffene Einrichtungen eine eigene Expertengruppe IT-Sicherheit ins Leben rufen, sofern das noch nicht geschehen sei, betonte Dr. Kurt Marquardt von der RHÖN-KLINILUM AG: „Ohne wird es künftig nicht mehr gehen." Diese Gruppe kann dann auch die Kontaktstelle an das BSI benennen. Es sei nicht ratsam, damit bis 29. Dezember 2017 zu warten, so Marquardt. Denn erst mit der Benennung einer Kontaktstelle erhält eine Einrichtung regelmäßige Informationen des BSI und ist in alle KRITIS-relevanten Kommunikationsprozesse eingebunden.

„Geld kann nicht aus DRG-Erlösen kommen"

Die Kontaktstelle muss 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr erreichbar sein. Ihre Aufgabe besteht unter anderem darin, „erhebliche" Störungen an das BSI zu melden. Je nach Schweregrad der Störung erfolgt die Meldung anonym oder unter Nennung der Einrichtung. In jedem Fall wird die meldende Einrichtung nicht öffentlich genannt: „Die Unternehmen müssen uns vertrauen, sonst wird es nicht funktionieren", betonte Matthias Fischer.

Eine der Gretchenfragen beim Thema Meldepflicht ist natürlich, was genau unter einer „erheblichen" Störung zu verstehen ist. „Erheblich ist ein unbestimmter Rechtsbegriff, und es wird Aufgabe des BSI sein, das auszulegen", so Fischer vage. Zumindest am Anfang dürfte „erheblich" unter anderem daran festgemacht werden, welcher Anteil der jeweiligen Versorgungskapazitäten von einer Attacke betroffen ist. Fischer gab allerdings zu, dass hier möglicherweise noch Konkretisierungsbedarf bestehe. Er verwies auch darauf, dass im Jahr 2019 eine Evaluation des Gesetzes vorgesehen sei. Die Option, nachzujustieren, wurde also von vornherein eingeplant.

Eng mit der Kontaktstelle in Zusammenhang steht die Frage der Finanzierung der KRITIS-Anforderungen. Mit einer einzelnen neuen Stelle in der IT-Abteilung, so der Tenor in Berlin, werde ein KRITIS-Krankenhaus nicht auskommen, von den Aufwänden für die Auditierung und die Umsetzungen der technischen Anforderungen gar nicht zu reden.

Als erstes seien jetzt konkrete Kostenschätzungen nötig, damit klar sei, um welche Beträge es überhaupt gehe, betonte Neuhaus: „Das Geld kann in jedem Fall nicht aus den DRG-Erlösen kommen, und es wird eher auch nicht aus den Investitionsmitteln der Länder kommen, die ohnehin nicht mehr aufgestockt werden." Gespräche mit der Politik über eine Refinanzierung nach erfolgreicher Umsetzung liefen. Konkrete Ergebnisse gebe es aber noch nicht, und Zusagen seien noch von niemandem getroffen worden.

Öffnung versus Sicherheit

Das eigentliche Megathema bei der Umsetzung der BSI-Kritisverordnung ist aus Sicht der großen Krankenhäuser und auch aus Sicht der DKG weder die Finanzierung noch die Ausgestaltung eines branchenspezifischen Sicherheitsstandards noch die Frage, wie „erhebliche" Störungen definiert werden. Das Megathema ist vielmehr die IT-

» Manche hoffen, dass der branchenspezifische Sicherheitsstandard zu einer Art Dominoeffekt führt, der die IT-Sicherheit im Gesundheitswesen flächendeckend verbessert.«

Sicherheit in all jenen Einrichtungen, die nicht unter die Verordnung fallen.

Marquardt sieht die Krankenhäuser letztlich zwischen allen Stühlen. Einerseits werde gefordert, hohe Sicherheitsanforderungen umzusetzen. Andererseits zielten viele Gesetze der vergangenen Jahre und auch viele Förderprojekte des Bundes, etwa das Förderprojekt Medizininformatik, explizit auf die Öffnung einst abgeschotteter IT-Systeme. Die größeren Krankenhäuser, die die BSI-Kritisverordnung erfüllen müssen, fürchten, dass sie sich mit dieser politisch erzwungenen Öffnung zusätzliche IT-Risiken einkaufen, die irgendwann nicht mehr beherrschbar sind, wenn die im Rahmen von zum Beispiel Allianzakten kooperierenden Einrichtungen nicht ihrerseits hohe Sicherheitsstandards haben. „Über 90 Prozent der Krankenhäuser sind in Sachen Sicherheit weitgehend blank. Sie haben weder das nötige Fachpersonal noch die nötigen Komponenten“, so Marquardt.

Am Beispiel der RHÖN-KLINIKEN illustrierte der IT-Experte, wo derzeit überall die Schotten geöffnet werden. Neben den Allianz- und Fallakten, die mittlerweile zu einem der wichtigsten Prozessthemen überhaupt geworden seien, gebe es Projekte, bei denen Patienten im Rahmen des (politisch angestoßenen) Entlass-managements mit Sensoren ausgestattet werden. Die müssten zumindest indirekt mit dem Klinikarchiv kommunizieren und öffneten auf diese Weise eine Eintrittspforte. Auch das Cognitive Computing führe zu einer Öffnung der Kommunikation, zumindest dann, wenn es dazu genutzt werde, auf internationale Wissensquellen zuzugreifen.

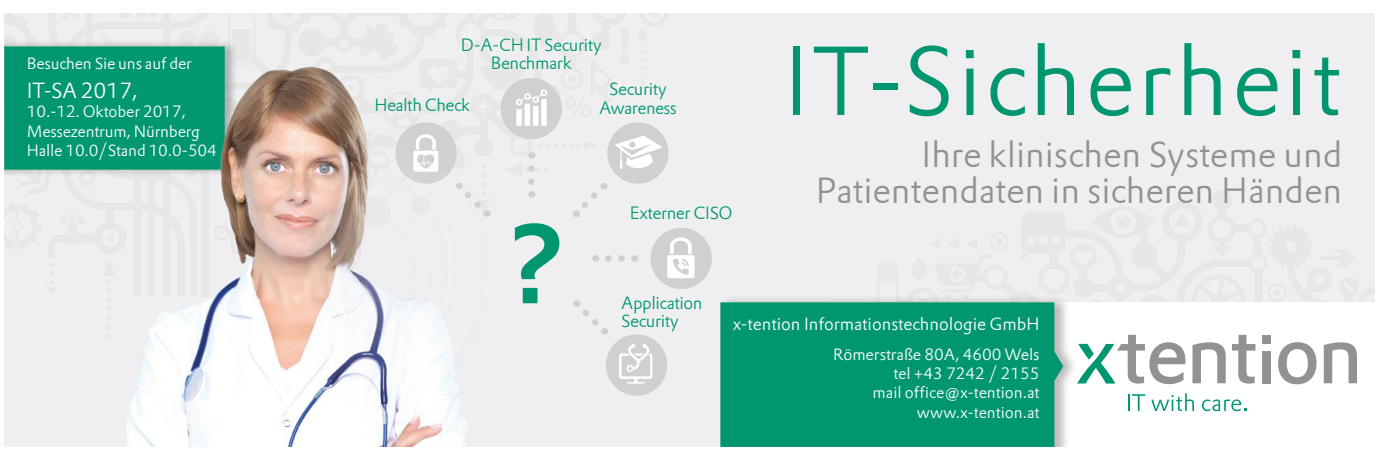
„Gesetz kommt zur rechten Zeit“

Fischer hofft vor diesem Hintergrund, dass der branchenspezifische Sicherheitsstandard zu einer Art Dominoeffekt führt, der letztlich die IT-Sicherheit im Gesundheitswesen flächendeckend verbessert: „Sich an den Stand der Technik bei der IT-Sicherheit zu halten, ist schon jetzt aus zivilrechtlicher Sicht erforderlich“, so Fischer. Wenn etwas passiere, dann sei das Krankenhaus in der Haftung, egal ob es unter die BSI-Kritisverordnung falle oder nicht: „Wenn der Branchenstandard existiert, wird er zum Sorgfaltsmaßstab, und jeder Richter wird fragen, warum er nicht eingehalten wurde.“

Zu sehr verlassen auf die im KRITIS-Verfahren zu definierenden technischen Standards sollte sich jedoch niemand. IT-Sicherheit hat auch eine große organisatorische Komponente, nicht nur bei der Abwehr von Gefahren, sondern auch beim Umgang mit Zwischenfällen, zu denen es natürlich immer kommen kann. Im RHÖN-KLINIKUM Gießen-Marburg erstellt eine eigene Arbeitsgruppe derzeit einen Plan, wie das Haus im Falle eines Falles komplett ohne (Standard-)IT betrieben werden kann. Es werden Reserverechner für einzelne Aufgaben aufgebaut und es werden Systeme definiert, die auch ohne Netzanschluss arbeiten können. „Wir müssen auch organisatorisch mächtig nachlegen“, so Marquardts Fazit. „Das Gesetz sensibilisiert die, die sich um IT-Sicherheit noch nie gekümmert haben, und kommt insofern zur rechten Zeit.“ ■

PHILIPP GRÄTZEL VON GRÄTZ
ist Chefredakteur der E-HEALTH-COM.

ANZEIGE



Interview
SICHERES ENTWICKELN VON MEDIZINGERÄTEN

Was müssen Medizintechnik-Hersteller beachten, damit ihre Produkte heute gegen Angriffe von außen gut geschützt werden? Zentral für ein sicheres Entwickeln ist dabei der Austausch mit IT-Entwicklern, Forschern und professionellen Hackern, verrät Hannes Molsen, Product Security Manager bei Dräger, im Interview mit E-HEALTH-COM.

Medizintechnische Geräte werfen aktuell die Frage der Sicherheit auf, wenn sie in einem klinischen Netzwerk betrieben werden. Mit zunehmenden Hackerangriffen wächst die Furcht bei Klinikbetreibern, ärztlichem Personal und Patienten, dass Cyberangriffe nicht nur die Verwaltung sondern auch die Therapie ins Visier nehmen könnten. Nach Ansicht von Hannes Molsen, der als Global Product Security Manager für die IT-Sicherheit von Dräger-Produkten zuständig ist, kann die Medizintechnik heute gegen Angriffe von außen gut geschützt werden. Allerdings sollten sowohl die Klinik als auch die Hersteller ein möglichst hohes Sicherheitsniveau beim Betreiben und Inverkehrbringen von medizinischen Geräten anstreben. Für den Sicherheitsexperten bedeutet das auch, über mögliche Schwachstellen zu reden und Hard- und Software-Lösungen auch mithilfe von Dritten zu entwickeln.

Beim Thema IT-Sicherheit sind Kliniken und Hersteller gleichermaßen angesprochen. Was kann ein Krankenhaus hier tun?

Jeder wünscht sich natürlich völlige Kontrolle, insbesondere in sensiblen Klinikbereichen wie auf einer Intensivstation. Und die Klinikbetreiber achten auf hohe Sicherheitsstandards. Das fängt bei Zugangskontrollen zu den Medizingeräten an, führt über regelmäßige Virenscanner- und Software-Updates bis hin zu abgeschirmten Netzwerken, in denen beispielsweise Anästhesie- und Beatmungsgeräte betrieben werden. Außerdem gehört die IT auch zum klinikweiten Risikomanagement.

Muss ich mir als Arzt oder Patient keine Sorgen machen?

Klinikmitarbeiter müssen sensibel sein im Umgang mit IT. Nicht alle Risiken sind beherrschbar. Langsam setzt sich aber das Bewusstsein durch, dass zum Beispiel ein USB-Stick nicht nur Daten von einem Gerät zum anderen übertragen kann, sondern potenziell auch Überträger einer verborgenen Schadsoftware sein kann. Auch die Hersteller sind dabei, umzudenken. Geräteparks in den Kliniken sind heterogen mit modernen Medizingeräten aber auch älteren Komponenten. Vor zehn oder mehr Jahren herrschte natürlich noch ein anderer Sicherheitsfokus vor. Damals stand der technisch zuverlässige Betrieb im Netzwerk im Vordergrund, und weniger Vorkehrungen gegen das vorsätzliche oder unbeabsichtigte Manipulieren. Inzwischen achten die Hersteller sensibler auf potenzielle Sicherheitslücken. Mit dem Thema IT-Sicherheit im Krankenhaus müssen also sowohl Betreiber als auch Hersteller bewusst umgehen. Dann kann das Risiko für Störungen möglichst gering gehalten werden.

HANNES MOLSEN
ist Global Product Security Manager bei Dräger.

»Vor allem der Austausch mit IT-Entwicklern, Forschern und „White Hat"-Hackern hat uns vorangebracht.«

Was können Sie als Hersteller tun?
Hundertprozentige IT-Sicherheit kann heute niemand garantieren. Auch wenn wir beim Entwickeln neuer Geräte stets potenzielle Lücken simulieren und dadurch möglichst ausschließen. Um das Risiko für Störungen zu minimieren, ist es für uns daher auch wichtig zuzuhören. Wie einige andere Hersteller auch, haben wir eine Extraseite für Produktsicherheit mit einem „Coordinated Disclosure Statement" auf der Dräger-Webseite (http://static.draeger.com/security/) eingerichtet. Dort können Anwender, Entwickler oder IT-Sicherheitsforscher erkannte oder mögliche Schwachstellen bei Dräger-Geräten melden. Wir öffnen damit einen Kanal zu Fans und Kritikern von Dräger, aber auch neutralen Dritten, die uns so wichtige Hinweise geben können, was wir vielleicht noch besser machen können.

Zudem treten wir aktiv in den Dialog zu unseren Kunden. Als Mitte Mai 2017 die Ransomware „WannaCry" weltweit Millionen Rechner in Krankenhäusern, Universitäten, Unternehmen und Behörden infizierte, prüften wir, inwieweit Dräger-Medizingeräte mit Windows-Betriebssystemen davon betroffen sein könnten. Das Ergebnis unserer Untersuchung veröffentlichten wir anschließend als offenen Brief auf unserer Seite und konnten so für etwas Beruhigung sorgen.

Was haben Sie denn aus dem „Zuhören" gelernt?
Vor allem der Austausch mit IT-Entwicklern, Forschern und „White Hat"-Hackern hat uns vorangebracht. Letztere suchen gezielt Schwachstellen in Software und Geräten, um diese präventiv mitzuteilen. Darüber hinaus gibt es internationale Organisationen wie „I Am The Cavalry", die es sich zum Ziel gesetzt haben, mit Computertechnologien kritisch und sicherheitsbewusst umzugehen. Hier diskutieren weltweit IT-Experten, wie die zunehmende Digitalisierung unseres Zusammenarbeitens, die unser Leben und die öffentliche Sicherheit direkt beeinflusst, sicher ablaufen kann. Ich habe mich außerhalb meiner beruflichen Aufgaben dazu entschlossen, Teil dieses Netzwerks zu werden.

Im nächsten Schritt geht es darum, diese Erkenntnisse in die Entwicklung und Fertigung zu integrieren. Dazu haben wir vor einiger Zeit einen sicheren Entwicklungsprozess eingeführt. Wir geben uns als Unternehmen eigene Sicherheitsvorgaben, die beim Design neuer Produkte, bei ihrer Produktion sowie später im Betrieb beim Kunden greifen. Dazu gehört es beispielsweise, Medizingeräte mit einem möglichst hohen Sicherheitsstandard auszuliefern, sie gegen nichtautorisierte Zugriffe zu schützen und ihre Betriebssysteme zu „härten". Das heißt etwa, dass wir unnötige Software-Bestandteile weglassen und so mögliche Angriffspunkte von vornherein begrenzen.

Dräger verfolgt darüber hinaus eine Strategie, bei der Medizinprodukte im ersten Fehlerfall, also beispielsweise dem Ausfall des Datennetzes, eigensicher sind: Sie funktionieren in diesem Fall autark weiter. „Sicherheit" ist bei Dräger ein ganzheitliches Konzept und umfasst mehrere Ebenen zur Sicherung der medizinischen Grundfunktionalität.

© DRÄGER

Testen Sie die IT-Sicherheit, bevor Ihre Geräte auf den Markt kommen?
Viele Unternehmen gehen dazu über, netzwerkfähige Produkte probeweise hacken zu lassen, bevor sie in den Markt eingeführt werden. Auch wir arbeiten mit professionellen Hackern zusammen, wobei viele neue Produkte bereits in der frühen Entwicklungsphase und später auch mehrmals bis zur Marktreife auf den Prüfstand kommen. So wollen wir Überraschungen vermeiden. Zum Beispiel könnte das Korrigieren eines spät entdeckten Software-Fehlers sehr viel Aufwand verursachen, wenn dazu die längst gelegte Plattform noch einmal angefasst werden müsste. Externe helfen uns so, nicht nur die Sicherheit unserer Produkte zu optimieren, sondern auch durch möglichen Mehraufwand entstehende Kosten zu vermeiden.

Wie neu ist der „sichere Entwicklungsprozess"?
Die Idee des sicheren Entwickelns ist nicht neu. Einer der prominentesten Begründer dieser Vorgehensweise ist Microsoft mit dem Security Development Lifecycle, einem frei verfügbaren Prozess, um Sicherheit der Microsoft-Produkte zu verbessern (https://www.microsoft.com/en-us/sdl/). Wir haben dies für uns adaptiert, weil wir die Vorteile der Fehlervermeidung in verschiedenen Produktphasen erkannt haben. Der „sichere Entwicklungsprozess" bei Dräger fußt auf dem kontinuierlichen Training und der Weiterbildung der Mitarbeiter in Sachen IT-Sicherheit. Er beginnt bereits im Stadium des Produkt-Entwurfs, über die eigentliche Entwicklung und das Penetrieren der Sicherheitsmerkmale, bis hin zum Einführen des Produkts in den Markt. Auch das weitere Versorgen mit Sicherheits-Updates über die Lebensdauer der Komponenten gehört zu diesem Prozess.

Können Kliniken, die sicher entwickelte Geräte einsetzen, sich künftig stärker zurücklehnen?
Ziel ist es, die Hürde für bewusst verursachte Störungen so hoch wie möglich zu halten und damit die Medizintechnik als Angriffspunkt unattraktiv zu machen. Wir sehen uns dabei als Hersteller in der Rolle eines Unterstützers. Wie helfen Kliniken, ihre Verantwortung als Betreiber vernetzter Medizingeräte wahrzunehmen. Dadurch, dass Geräte immer sicherer werden, wird es auch für die Krankenhäuser leichter, einen sicheren Betrieb zu gewährleisten. Sicherheitsmerkmale des Herstellerprodukts müssen dabei zu der vorhandenen Sicherheitsausrüstung der IT des Kunden passen, um optimal integriert werden zu können. Mit zunehmend sicherer werdenden Krankenhausinfrastrukturen können die Potenziale gemeinsam mit den Herstellern immer besser ausgenutzt werden. Sicherheit bei vernetzten Medizingeräten ist also beides, die Schutzmechanismen der Geräte selber und ihre Einbindung in eine sicher betriebene Umgebung in der Klinik. Ein Hersteller muss die strukturellen Voraussetzungen auf Klinikseite beachten und hat deswegen nicht alleinig Einfluss darauf, wie sicher ein Medizinprodukt in der jeweiligen Umgebung ist.

Da kommen wir auf das Eingangsthema zurück, die Sicherheitsstandards in den Kliniken …
Genau, hierbei ist zum Beispiel ein Risikomanagement, das medizinische IT-Netzwerke (MIT) mit einschließt, eine sinnvolle Grundlage. Es ergänzt die Sicherheitsanstrengungen der Hersteller auf Klinikseite. Um die Sicherheit von MITs zu erhöhen, verabschiedete die InternationalElectrotechnical Commission (IEC) 2010 die Norm IEC 80001-1; die deutsche Fassung DIN EN 80001-1 folgte ein Jahr später. Diese Norm „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten" gibt Standards für die Risikoanalyse und den Unterhalt medizinischer IT-Netzwerke vor. Sie beschreibt, wie Server, Medizinprodukte oder mobile Endgeräte in einem medizinischen IT-Netzwerk) sicher und störungsfrei miteinander kommunizieren können. Dazu muss beispielsweise vorab geprüft werden, wie nahtlos sich Medizinprodukte in die bestehende Gerätelandschaft einfügen lassen. Mögliche Netzausfälle – und hier müssen nicht nur Hackerangriffe, sondern auch außergewöhnliche Ereignisse wie Unwetterschäden ins Kalkül gezogen werden – sollten von einem Risikomanager antizipiert und mit einem Notfall-Fahrplan belegt werden. Die Norm empfiehlt darüber hinaus, Verantwortlichkeiten festzulegen, einen Risikomanager zu benennen und einen Risikomanagement-Prozess in Gang zu bringen. Die Krankenhausleitung sollte außerdem dafür sorgen, dass die Beteiligten geschult werden und sich regelmäßig austauschen. Viele Häuser sehen offenbar eine Notwendigkeit von mehr Schulungen in diesem Bereich: Laut Krankenhausbarometer 2013 stufen über 70 Prozent der befragten Kliniken Fortbildungen zum Risikomanagement für den ärztlichen Dienst als „wichtig" bis „sehr wichtig" ein. ■

WORLD FORUM FOR MEDICINE

MEDICA®

13 – 16 NOVEMBER 2017
DÜSSELDORF GERMANY

www.medica.de

MEDICA CONNECTED HEALTHCARE FORUM
www.medica.de/MCHF1

MEDICA HEALTH IT FORUM
www.medica.de/MHIF1

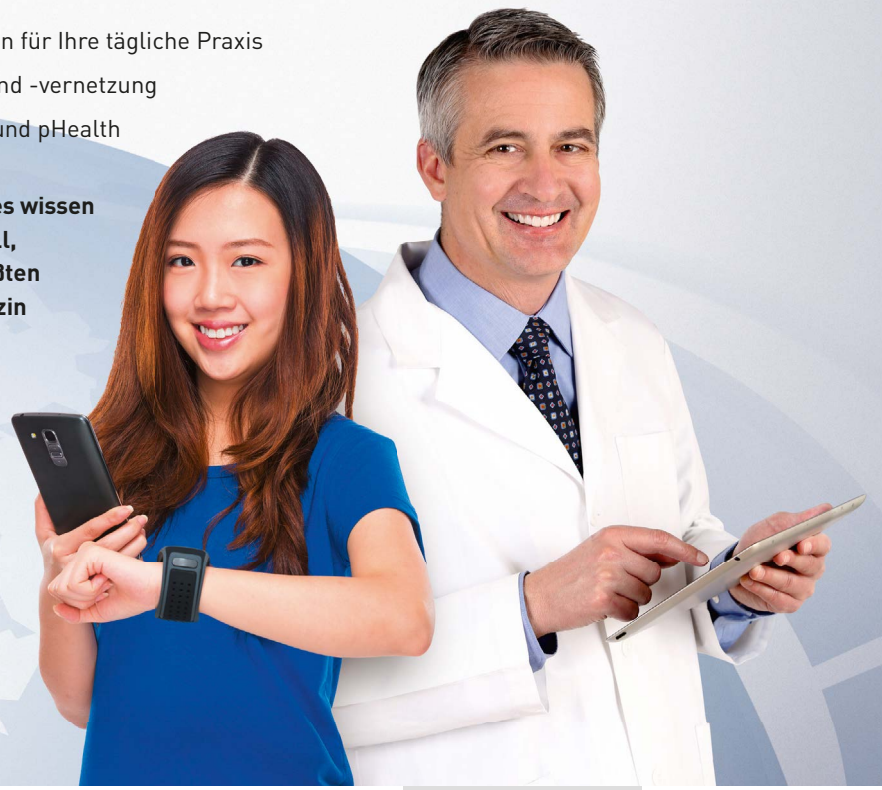
MEDICA ACADEMY
www.medica.de/MA1

T5 CAREER FORUM
www.medica.de/MCF1

Die Welt der medizinischen IT auf einen Blick:

- alle Neuheiten der medizinischen Informations- und Kommunikationstechnik
- exzellentes Wissen
- innovative Lösungen für Ihre tägliche Praxis
- Datengewinnung und -vernetzung
- eHealth, mHealth und pHealth und vieles mehr

Wer alles sehen, alles wissen und alles erleben will, der kommt zum größten Weltforum der Medizin nach Düsseldorf!



BE PART OF THE NO. 1!

Basis for Business

Messe Düsseldorf®

FÄLSCHUNGEN MIT E-SIEGELN VON SECRYPT BEGEGNEN

Ab sofort ermöglicht die secrypt GmbH die Erstellung elektronischer Siegel, mit denen sich Dokumente wirksam vor unbemerkten Fälschungen schützen lassen. Für die Nutzung der E-Siegel haben die Signaturexperten einige Tipps zusammengestellt.

Medizinische Einrichtungen können die Integrität und Authentizität ihrer digitalen Dokumente nun gemäß der EU-Verordnung eIDAS mit einem rechtssicheren digitalen Stempel nachweisen. Abhängig vom jeweiligen Dokumentenvolumen und vom Grad der Prozessautomatisierung kommen hierbei folgende Möglichkeiten in Betracht:

Zum einen lässt sich das elektronische Siegel manuell über die Signatursoftware digiSeal® office der secrypt GmbH auf einzelne Dokumente aufbringen. Hierbei ist die PIN der Siegelkarte bei jedem Siegelvorgang erneut einzugeben. Daher eignet sich die Lösung vor allem dann, wenn nur ab und zu einige wenige Dokumente, z.B. innerhalb einer Arztpraxis, zu siegeln sind. Alternativ erlaubt digiSeal® office pro das Siegeln mehrerer Dokumente in einem Stapel – bei nur einmaliger PIN-Eingabe für die Multi-Siegelkarte.

E-Siegelung am Einzelarbeitsplatz mit digiSeal® office.

Für hochvolumigere Prozesse mit Tausenden und Millionen von Dokumenten, die z.B. in einer Klinik erstellt werden, kommt der Siegelserver digiSeal® server von secrypt zum Einsatz. Dieser ermöglicht die hochperformante automatisierte zentrale Siegelerzeugung. Da das Siegelzertifikat für die gesamte Organisation gilt und nicht mehr an eine Einzelperson gebunden ist, können mehrere Mitarbeiter darauf zugreifen. Um sicherzustellen, dass nur berechtigte Mitarbeiter und Prozesse das E-Siegel auslösen, sind Zugriffsrechte im Signaturserver zu hinterlegen.

Mit dem elektronischen Stempel lassen sich ganze Papierarchive, aber auch die Eingangspost rechtssicher nach TR RESISCAN digitalisieren. Der digiSeal® server bringt das E-Siegel einfach nach Abschluss des Scanvorganges automatisch auf das Digitalisat auf. Somit muss der Scan-Operator seine Signatur-PIN nicht mehr für jedes digitalisierte Dokument einzeln eingeben. Zudem genügt ein Siegelzertifikat auf einer Multi-Siegelkarte – Signaturkarten für jeden einzelnen Scan-Operator sind nicht mehr erforderlich.

Und auch originär digitale Dokumente, darunter Entlassbriefe, unkritische Laborbefunde, pflegerische Dokumentationen und Rechnungen, lassen sich mit dem starken Integritätsschutz versehen und so vor unbemerkten Fälschungen schützen. Anschließend können sämtliche digitale Dokumente im elektronischen Archiv abgelegt werden.

„Das elektronische Siegel beschleunigt digitale Dokumentenprozesse und hilft, das Papieraufkommen auf äußerst komfortable Weise und europäisch rechtsverbindlich weiter einzuschränken. Bei uns erhalten Kunden alles aus einer Hand: von der Beratung, über die Signatursoftware und die Siegelkarte bis hin zum Kartenleser“, sagt Tatami Michalek, Geschäftsführer der secrypt GmbH. ■

SECRYPT GMBH
Tatami Michalek,
Geschäftsführer der secrypt GmbH
Bessemerstr. 82, 12103 Berlin
Tel.: +49 - (0)30-756 59 78-0
mail@secrypt.de
www.secrypt.de

EINFACH SICHER

Mit der zunehmenden Digitalisierung in Krankenhäusern vergrößert sich die Angriffsfläche für Hacker, und die Gefahr von Cyberattacken steigt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt daher neuerdings erhöhte Sicherheitsanforderungen an Kliniken. Wie ein wirksamer und kostengünstiger Schutz in der Praxis aussehen kann, zeigt ein Beispiel der Telekom.

Die aktuelle Änderungsverordnung des seit 2015 geltenden IT-Sicherheitsgesetzes verpflichtet Krankenhäuser unter anderem dazu, ihre IT nach dem Stand der Technik angemessen abzusichern und diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen. Erhebliche IT-Störungen sind zudem umgehend an das BSI zu melden. Die neuen Regeln gelten allerdings nicht für alle Einrichtungen in Deutschland: Angesprochen sind nur die 110 größeren Krankenhäuser und Kliniken, die mindestens 30 000 Behandlungsfälle im Jahr vorweisen. Gleichwohl dürften dadurch De-facto-Standards für die Branche gesetzt werden, so dass sich künftig auch Einrichtungen daran messen lassen müssen, die nicht in den Geltungbereich des Sicherheitsgesetzes fallen.

Achillesverse Digitalisierung

Dass die strengen Auflagen des BSI berechtigt sind, zeigen die Hackerangriffe der letzten Monate. Zuletzt legte im Mai 2017 eine weltweite Attacke rund 40 Krankenhäuser in Großbritannien lahm, weil ein Computervirus die Daten der IT-Systeme blockierte und die Erpresser ein Lösegeld für deren Freigabe verlangten. Ein Angriff, der längst kein Einzelfall mehr ist.

„Cloud, Mobile Computing oder das Internet der Dinge gehören in Kliniken heute zum Alltag“, sagt Timo Baumann, Leiter Business Development bei Telekom Healthcare Solutions. „Statt mit Papierakten gehen Ärzte heute mit iPads zur Visite und greifen über die mobilen Geräte direkt am Patientenbett auf Befunde und Untersuchungsergebnisse zu. Das erleichtert und verbessert zwar auf der einen Seite die Arbeit von Medizinern und Pflegepersonal, erhöht aber auf der anderen Seite das Risiko für Cyberangriffe.“ Kurz: Wer digitale Lösungen einsetzt, muss sie auch entspechend schützen. Doch hier hapert es. Vielfach beschränken sich die Sicherheitssysteme in Kliniken auf Antivirenprogramme und Firewalls. Der Grund: Viele Einrichtungen scheuen die Implementierung einer Security-Lösung, weil ihnen das sehr spezielle Know-how rund um Bedrohungsszenarien und funktionierende Abwehrmechanismen fehlt.

Angriffe erkennen, bevor sie Schaden anrichten

Dabei muss ein wirksamer Schutz weder komplex noch aufwändig sein: Ein Sicherheitsinformations- und Ereignis-Management (SIEM), wie es die Telekom gemeinsam mit ihrem Partner AlienVault anbietet, erkennt mögliche Attacken, noch bevor sie Schaden anrichten können.

Dazu sammelt es Millionen von sicherheitsrelevanten Daten, setzt diese miteinander in Beziehung und erkennt daraus in Echtzeit bestimmte Muster. Sobald auffällige Abweichungen vom Normalzustand auftreten, löst das System einen Alarm aus. IT-Experten können so bereits zu einem sehr frühen Zeitpunkt Gegenmaßnahmen ergreifen. Die Telekom betreibt die Lösung auf Wunsch in einem ihrer hochsicheren deutschen Rechenzentren und steuert sie von einem Security Operations Center aus. Für das Klinikum selbst ist der Installations- und Betriebsaufwand daher gering. ■

Weitere Informationen finden Sie unter:
https://www.telekom-healthcare.com/de/kliniken/outsourcing-betrieb/it-sicherheit/cyber-defense-406334

Kontakt:
Timo.Baumann@t-systems.com

MAKE ARCHIVING GREAT AGAIN

Ransomware: Datenschutz jenseits von Back-ups

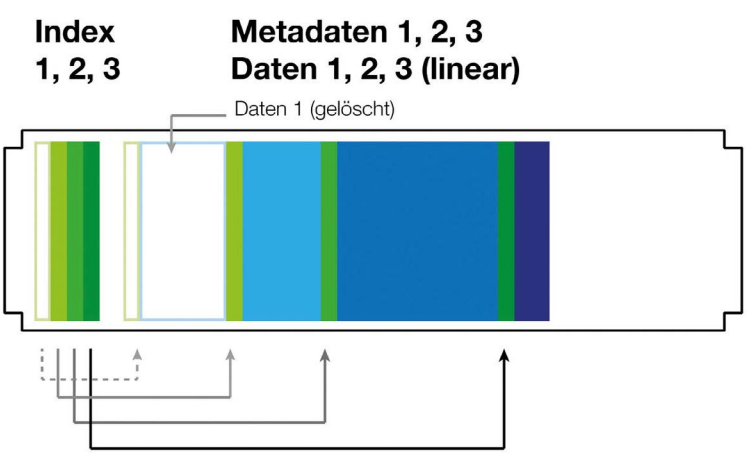
Inzwischen sind Archive zu großen Teilen digital. Damit lassen sich Lagerplatz, Workflows und Zugriffszeiten optimieren, gespeicherte Daten stehen jederzeit zur Verfügung. Die ständige Verfügbarkeit führt allerdings auch zur Angreifbarkeit, z.B. durch Ransomware.

Rechtlich relevante Datensätze wie Röntgenaufnahmen liegen zu großen Teilen auf revisionssicheren WORM-Speichern und sind damit vor jeglicher Manipulation geschützt – zumindest, wenn es sich um echte Hardware-WORM-Versiegelung handelt. Dennoch werden immer mehr Fälle bekannt, in denen Krankenhäuser und andere Einrichtungen vor großen Problemen durch Angriffe von Krypto-Trojanern stehen.

Da ein hundertprozentiger Schutz vor solchen Angriffen laut mancher Experten inzwischen Utopie ist, gilt es, sich vor den Folgen zu schützen. Die unmittelbare Folge ist meist eine Einschränkung des laufenden Betriebs, da auf wichtige Datensätze nicht mehr zugegriffen werden kann. Existiert eine vollumfängliche Back-up-Strategie für alle Daten, besteht zumindest die Möglichkeit, Daten wiederherzustellen und damit den Betrieb wieder aufzunehmen.

Betroffen sind Primärdaten, die nicht revisionssicher und auf WORM-Datenträgern gespeichert sind, sowie zunehmend statische Daten auf File-Servern, die aufgrund der schieren Menge nicht durch den ständigen Back-up-Prozess gesichert sind. Gerade im Gesundheitswesen fallen überproportional große Datenmengen an, die nicht alle auf WORM-Speichern wie den Silent Cubes gesichert sind. Würden ständig alle Daten in Back-ups fließen, verlängerte dies das notwendige Back-up-Fenster. Eine zeitnahe Sicherung wäre dadurch oft nicht gewährleistet, was bei Befall durch Viren wiederum Datenverlust zur Folge hätte. Zudem sorgt ansteigender Back-up-Bedarf nicht selten zu enorm wachsenden Lizenzkosten.

Zwischen dem Primärspeicher, der weiterhin ständig und idealerweise sogar kontinuierlich durch Back-ups geschützt sein muss, und dem revisionssicheren Archiv bietet sich deshalb eine weitere Speicherstruktur an: das aktive Archiv mit integrierter Datensicherung. Dabei wird durch lineare Datenstruktur, die mit Erasure Coding vierfach gegen Ausfall geschützt ist, ein Überschreiben und damit Manipulation wirksam verhindert. Neue Versionen einzelner Dateien, wie sie z.B. durch eine Verschlüsselung entstehen, überschreiben nicht mehr die vorherigen, intakten Versionen. Als Folge kann die intakte Vorversion jederzeit und unkompliziert mittels „Continuous Snapshot“ wiederhergestellt werden. Anders als „normale“ NAS-Speicher sind Daten auf solchen aktiven Archiven, wie z.B. dem SecureNAS auf Silent Bricks, also auch ohne WORM-Versiegelung vor Datenverlust durch Ransomware geschützt. ■



Die struktursichere, lineare Datenspeicherung auf Festplatten oder SSDs erlaubt es, jederzeit zu Vorversionen zurückzukehren.

FAST LTA AG
Rüdesheimer Str. 11, 80686 München
Tel.: +49-(0)89-89 047-0
info@fast-lta.de
www.fast-lta.de

WIE SICHER IST MEIN KRANKENHAUS?

Cybersicherheit an der Schnittstelle zwischen Medizintechnik und IT ist ein notorisch schwieriges Thema. Vasgard erhebt umfassend den Ist-Zustand und implementiert Lösungen.

MICHAEL PÖHLSEN
ist Geschäftsführer der Vasgard GmbH.

Wie ist es um die Cybersicherheit der Medizintechnik in meinem Krankenhaus bestellt?“ Diese Frage stellen sich Geschäftsführer und Medizintechnik- sowie IT-Leiter immer häufiger, seit regelmäßig neue Sicherheitslücken durch die Fachpresse gehen.

Schon ohne vernetzte Medizintechnik ist es schwierig genug, Krankenhaus-IT sicher zu betreiben. Die IT gleicht einem Gebäude mit zahlreichen Vorder- und Hinterausgängen, Kellertreppen und Fenstern, die alle gesichert werden müssen. Allein dies ist eine Aufgabe, bei der die meisten IT-Abteilungen an die Grenzen ihrer Ressourcen stoßen.

Hinzu kommt die vernetzte Medizintechnik – ein Ameisenhaufen, in dem kaum noch zu überschauen ist, durch welche minimale Änderung des Systems wieder neue, ungesicherte Ein- und Ausgänge entstehen. Einer stringenten Analyse und Überwachung stehen auch unklare Zuständigkeiten im Weg: Sind Medizintechniker oder ITler für die Cybersicherheit der Medizingeräte verantwortlich?

Zudem fehlt es in Krankenhäusern oft an Kompetenz. Kaum eine Institution verfügt über ausgewiesene Medizinprodukt-Integratoren, die sich an den Schnittstellen zwischen Medizintechnik und IT und in der DIN EN 80001 zu Hause fühlen. Eine Beschäftigung mit diesen Themen findet für IT- und Medizintechnik-Leiter oft zusätzlich zu ihren eigentlichen Aufgaben – und nach Feierabend – statt.

Michael Pöhlsen, Geschäftsführer der Vasgard GmbH, sichert mit seinem Team seit 2010 komplexeste IoT-Netzwerke in Branchen mit den höchsten Anforderungen an Informationssicherheit, wie Gesundheits- und Sozialwesen sowie dem Bankensektor.

Herr Pöhlsen, wie entstehen Sicherheitslücken in medizinischen Netzwerken?
Hauptproblem ist die unzureichend abgesicherte Kommunikation zwischen Geräten. Protokolle in der Medizintechnik sind oft so entworfen, dass sie einen Befehl von außen einfach ausführen, ohne die Identität oder Berechtigung des Urhebers zu prüfen.

Welche Folgen können solche Sicherheitslücken haben?
Sie bieten ein Einfallstor sowohl für Viren und andere Malware als auch für Angreifer, die Patientendaten stehlen oder manipulieren wollen. Diese Angreifer sind oft wirtschaftlich motiviert, wie wir in unserem Whitepaper „Vernetzte Medizingeräte: PKI schafft Vertrauen“ zeigen, und können finanziellen Schaden in sechs- bis siebenstelliger Höhe verursachen. Vom Reputationsverlust für das Haus – und Risiken für die Patienten – ganz zu schweigen.

Wie kann man sich schützen?
Eine mathematisch sichere Methode, um Kommunikation im IoT abzusichern, ist die Public-Key-Kryptographie verbunden mit einer Public-Key-Infrastruktur (PKI). So weisen sich vernetzte Geräte durch Zertifikate eindeutig aus, die Datenübertragung erfolgt verschlüsselt und damit abhör- und manipulationssicher. Gleichzeitig kann eine PKI auch für die Zutrittskontrolle und zum Management von Berechtigungen und Identitäten im Personalbereich verwendet werden – etwa, damit Ärzte Anordnungen mit rechtssicheren digitalen Signaturen abzeichnen können. ■

Das Whitepaper „Vernetzte Medizingeräte: PKI schafft Vertrauen“ erhalten Sie kostenlos unter
www.vasgard.com/pki

VASGARD

VASGARD GMBH
Michael Pöhlsen, Geschäftsführer
Straßenbahnring 15, 20251 Hamburg
Tel.: +49-(0)40-209 33 14 60
info@vasgard.com, www.vasgard.com

HAND AUFS HERZ: WIE IST ES UM IHR SICHERHEITSNIVEAU BESTELLT?

Ganz gut? Verbesserungswürdig? Vielleicht doch nicht ganz auf dem neuesten Stand? Oder sogar lückenhaft? Niemand kann es sich heutzutage leisten, Risiken im Datenschutz oder der Informationssicherheit einzugehen.

Vor allem im Gesundheitswesen sind besondere Sicherheitsmechanismen zu ergreifen, um die Vertraulichkeit, Verfügbarkeit, Integrität und Rechtskonformität von Gesundheitsdaten und der IT-Infrastruktur entsprechend sicherzustellen. Eine Möglichkeit, dies zu erreichen, ist, ein Informationssicherheits-Managementsystem (ISMS) nach der international anerkannten Norm ISO/IEC 27001 einzuführen und zu betreiben. Meist braucht es dazu die Unterstützung von Experten. Als Spezialist in der Schließung von Sicherheitslücken im Gesundheits- und Sozialwesen positioniert sich der IT-Dienstleister x-tention. Zertifiziert nach ISO/IEC 27001:2013 bietet das Unternehmen jetzt ein neues Service an, um das Informationssicherheits-Managementsystem bei seinen Kunden zu integrieren.

ISO/IEC 27001 Compliance Check

„Ein erster Schritt ist es immer, die Konformität zur ISO/IEC 27001 festzustellen und die noch umzusetzenden Anforderungen aufzuzeigen. Dies wird im Zuge eines ISO/IEC 27001 Compliance Checks in mehreren Phasen durchgeführt“, beschreibt Michael Punz, CISO bei x-tention, die Herangehensweise.

Zur Erhebung der Ist-Situation hinsichtlich Informationssicherheit und Datenschutz aus Management-Perspektive führt x-tention im ersten Schritt einen halbtägigen IT Security Health Check inklusive D-A-CH IT Security Benchmark beim Kunden durch. Darauf aufbauend werden Dokumente, die die Anforderungen der ISO/IEC 27001 betreffen, gesichtet.

Detailprüfung

Auf Basis des IT Security Health Checks und der Dokumentensichtung prüft x-tention die Umsetzung der Anforderungen der ISO/IEC 27001 im Detail. Dazu wird die Umsetzung der Kernanforderungen der Kapitel 4 bis 10 (das grundlegende ISMS) sowie der Anforderungen aus den Kapiteln A.5 bis A.18 aus dem Annex A detailliert geprüft.

Auswertung der Ergebnisse

Aus den Ergebnissen des ISO/IEC 27001 Compliance Checks leitet x-tention praxistaugliche Abweichungen und Handlungsempfehlungen ab, die in einem Abschlussbericht zusammengefasst werden.

MICHAEL PUNZ
CISO bei x-tention

x-tention CISO Michael Punz ergänzt: „Kunden profitieren von unserer langjährigen Erfahrung bei der Umsetzung von Sicherheitskonzepten. Auf der it-sa 2017 gibt es die Möglichkeit, mit unseren Experten direkt in Kontakt zu treten. Wir freuen uns auf Ihren Besuch!“ ■

xtention
IT with care.

X-TENTION INFORMATIONS-TECHNOLOGIE GMBH
Römerstr. 80A, A-4600 Wels
Tel.: +43-(0)7242-2155
office@x-tention.at
www.x-tention.at

Health IT-Portal

IT-Lösungen im Gesundheitswesen. In einem Portal vereint.

Das Health-IT-Portal ist als umfangreicher Recherche- und Nachrichtenpool DIE PLATTFORM für alle Akteure der Branche

DIE BRANCHE
AUF EINEN KLICK

Nutzen Sie das Health-IT-Portal

ALS UNTERNEHMEN

Für Produkte und Dienstleistungen
Werden Sie Partner und bleiben Sie für die Interessenten der Branche präsent und aktuell

ALS ANWENDER

Für Information und Orientierung durch Vielfalt

www.health-it-portal.de

Halle 10 / Stand 413

itsa 2017

Die IT-Security Messe und Kongress
The IT Security Expo and Congress

FILESERVER MANAGEMENT SUITE

FILESERVER MANAGEMENT SUITE

Access Management Solution

- Transparente Berechtigungsverwaltung für Fileserver, SharePoint und Drittsysteme
- Monitoring & Autokorrektur von nicht autorisierten Veränderungen
- Auditsichere Protokollierung der Berechtigungsvergabe
- Self Sevice Portal für Fachabteilungen und Datenverantwortliche
- Profilbasierte Vergabe von Berechtigungen
- Berechtigungsmanagement ohne IT-Hintergrundwissen
- Entlastung im User Help Desk
- Skalierbar für weltweit verteilten Einsatz
- Integration in Drittsysteme über API

www.fileservermanagementsuite.com

Telefon: +49 (6151) 86 18 – 0
E-Mail: fms@bayoo.net

BAYOONET AKTIENGESELLSCHAFT