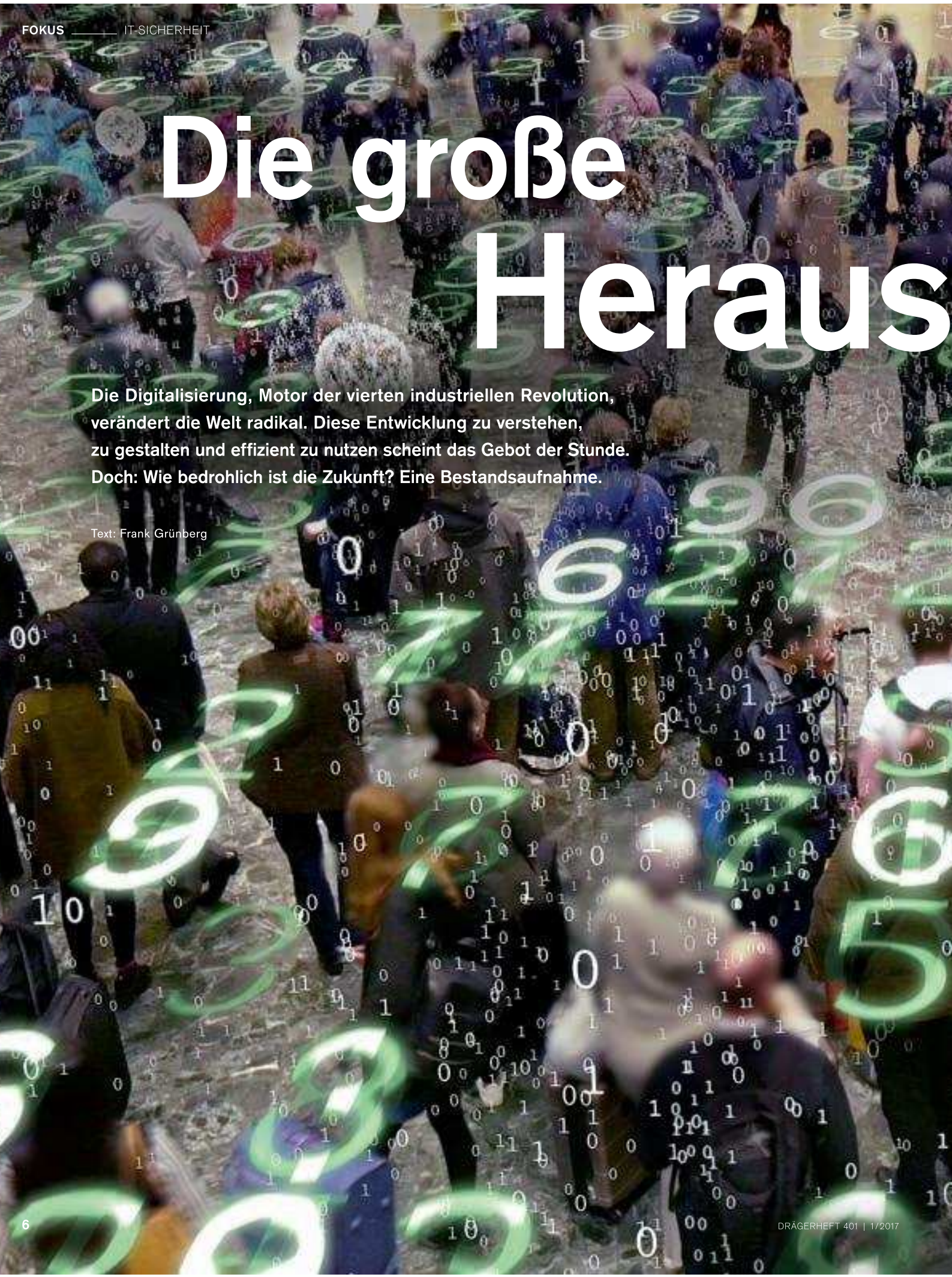
Die große Heraus

Die Digitalisierung, Motor der vierten industriellen Revolution, verändert die Welt radikal. Diese Entwicklung zu verstehen, zu gestalten und effizient zu nutzen scheint das Gebot der Stunde. Doch: Wie bedrohlich ist die Zukunft? Eine Bestandsaufnahme.

Text: Frank Grünberg



forderung

FOTO: PETER HOWELL/ISTOCKPHOTO

A

Apps, die Schritte zählen, zum Wassertrinken animieren und dabei helfen, mit dem Rauchen aufzuhören: Kleine Softwareprogramme, die sich auf mobilen Endgeräten nutzen lassen, sind für viele zum unverzichtbaren Begleiter geworden. Inzwischen soll es mehr als 100.000 Gesundheits-Apps geben. Nie zuvor war es möglich, persönliche Daten millionenfach – und ohne Zeitverzug – zu sammeln, zu analysieren und die Ergebnisse als Entscheidungshilfe zu nutzen. Der Vorteil von Big-Data-Analysen ist statistisch begründet: Je mehr Daten zur Verfügung stehen, desto besser lassen sich stabile Modelle zur Früherkennung von Krankheiten entwickeln und optimieren.

BIG DATA: MEHR ALS NUR VIELE DATEN

Die vierte industrielle Revolution ist gekennzeichnet von der Digitalisierung aller Produktions- und Arbeitsprozesse sowie der intelligenten Nutzung einer unvorstellbaren Menge an Daten. Wo aus dieser Quantität wieder eine neue Qualität wird, entsteht der Fortschritt. Zahlen und Fakten, die einige Aussichten eröffnen.

1697

Gottfried Wilhelm Leibniz entwickelt das Dualsystem, das Rechnen mit 0 und 1

1989

Das World Wide Web entsteht. Erst zur Kommunikation, dann auch für Kooperation, Steuerung, Überwachung und Produktion – etwa durch 3-D-Drucker

455 Exabyte*

kann ein Gramm menschlicher DNA codieren – denn auch die Vererbung ist digital

148

Milliarden US-$ war in etwa der Umsatz im Cloud Computing im Jahre 2016. Er soll 2017 um 25 % steigen

1.024 kHz

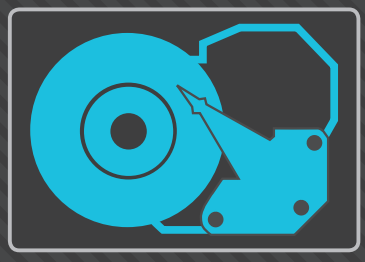
war die Taktrate des Computers, den Apollo 11 bei der ersten Landung eines Menschen auf dem Mond 1969 an Bord hatte. Er wog 32 Kilogramm und verbrauchte fast 2.000 Watt an Leistung. Die Taktrate eines heutigen Laptops liegt beim 4.000-fachen

3,7

Milliarden Menschen hatten im März 2017 Zugang zum Internet. Das ist rund die Hälfte der Weltbevölkerung

42.000

Exabyte* ist der Speicherbedarf für alles, was die Menschheit je gesprochen hat, digitalisiert mit 16 kHz/16 Bit



* Ein Exabyte sind eine Milliarde Gigabyte

FOTO: SHUTTERSTOCK; ILLUSTRATIONEN: PICFOUR; QUELLEN: BIBLIOTHECA AUGUSTANA, CERN, NEW SCIENTIST, WATERFORDTECHNOLOGIES, NASA, INTERNET WORLD STATS, UNIVERSITY OF PENNSYLVANIA

2019 will Deutschland die elektronische Patientenakte eingeführt haben

Blickfang: Mit einer Smartwatch hat man wichtige Vitalparameter immer im Blick, kann sie teilen, Trends erkennen und sein Verhalten danach optimieren

Mit den Chancen wachsen allerdings auch die Risiken, etwa hinsichtlich des Missbrauchs persönlicher Daten. Während das Angebot im privaten Sektor geradezu explodiert, stehen viele professionelle Gesundheitseinrichtungen erst am Anfang. Wie langsam die Mühlen dort mitunter mahlen, zeigt sich auch in Deutschland. Erst nach einigen Diskussionen trat hier Anfang 2016 das E-Health-Gesetz in Kraft, das erstmals einen detaillierten Fahrplan für die digitale Vernetzung von Ärzten, Apotheken und Krankenhäusern beschreibt – und ihn sogar mit finanziellen Anreizen verknüpft. Seit diesem Jahr erhalten niedergelassene Mediziner 55 Cent pro Arztbrief, wenn er elektronisch verschickt und mit ihrem Heilberufsausweis signiert wird. In Zukunft werden auch Sprechstunden und Befunde von Röntgenaufnahmen per Video vergütet. 2018 soll dann der Medikationsplan elektronisch von der Gesundheitskarte abrufbar sein, 2019 die elektronische Patientenakte eingeführt werden. Voraussetzung dafür ist eine eigene Telematik-Infrastruktur (TI) für das deutsche Gesundheitswesen, die in der letzten Ausbaustufe mehr als 70 Millionen gesetzlich Versicherten zugutekommen soll. Die Bundesregierung spricht in diesem Zusammenhang vom einem der weltweit größten IT-Projekte.

Zeitplan für Telematik-Infrastruktur bröckelt

Während Verbände und Behörden beim Thema Cyber-Security schon mal Tempo machen (siehe auch S. 11: „Wege aus der digitalen Geiselhaft“), bröckelt der Zeitplan. Der Termin für die Bereitstellung der TI wurde um ein Jahr verschoben. Ob das Management aller Versichertenstammdaten wie gefordert bis Mitte 2018 zustande kommt, scheint fraglich. Darüber hinaus ist der elektronische Heilberufsausweis bislang kein Verkaufsschlager, bei nicht einmal vier Prozent der niedergelassenen Ärzte war er Ende 2016 im Einsatz. Auch auf EU-Ebene erinnern die Versuche, mehr digitale Technik im Gesundheitswesen zu etablieren, nicht gerade an einen Hochgeschwindigkeitszug. Der grenzübergreifende „Action Plan“ blickt zwar bis 2020 und wurde bereits einmal um acht Jahre verlängert; ein Projekt widmete sich sogar der Aufgabe, den Austausch von Patientendaten zwischen den USA und Europa zu erleichtern. Aktuell scheinen viele Aktivitäten allerdings aufs Abstellgleis geraten zu sein. Wer auf den entsprechenden Webseiten danach sucht, muss sich mit mindestens zwei Jahre alten Meldungen zufriedengeben. Der „Ländervergleich E-Health“, den die deutsche Außenwirtschaftsagentur German Trade and Invest im November 2015 veröffentlichte, trägt viele Rahmendaten und Absichtserklärungen aus elf Ländern zusammen, jedoch wenig konkrete Projekte. Lichtblicke sind Estland, wo mittlerweile fast die gesamte Bevölkerung digital auf persönliche Gesundheitsakten zugreifen kann, oder Schweden, wo bereits gut die Hälfte der Akutkrankenhäuser mit anderen Akteuren des Gesundheitswesens vernetzt ist. In Südafrika wiederrum wird im Zuge des „MomConnect“-Projekts geprüft, welche Auswirkungen es hat, wenn sich Schwangere und junge Mütter per SMS kostenfrei an →

Stufe	Beschreibung	USA	EU	DK	D	I	NL	E	TR
7	Papierlose Umgebung, Datenkontinuität innerhalb des Hauses und mit anderen Pflegedienstleistern, analytische Organisationssteuerung, optimierte klinische operative und Geschäftsprozesseffizienz	4,2	0,3	0,0	0,7	0,0	2,9	0,0	0,2
6	Optimierte klinische Versorgung (z. B. Therapieprotokolle), geschlossener Medikationskreislauf, Kostenreduktion für Lagerhaltung und Transkription, verbesserte Abrechnung	27,1	2,5	0,0	0,0	2,2	8,6	6,3	2,1
5	Vermeidung von Duplikaten, Filmarchiv; Austausch und Zugriff	35,9	29,5	100,0	16,9	34,8	62,9	47,9	16,7
4	Fehlerreduktion bei klinischen Aufträgen/Medikationsverordnung	10,1	6,7	0,0	4,9	2,2	0,0	4,9	10,4
3	Optimierte Auftrags-Befund-kommunikation, klinische Dokumentation und Standardisierung der Pflege	16,4	5,3	0,0	9,2	1,5	0,0	2,8	7,7
2	Optimierter Zugang zu diagnostischen Ergebnissen und Arztbriefen	2,6	34,5	0,0	29,6	34,1	22,9	26,4	44,3
1	Optimiertes Fachabteilungsmanagement	1,7	7,9	0,0	1,4	18,5	2,9	2,1	8,4
0	Patientenadministration und Ressourcenmanagement	2,1	13,3	0,0	37,3	6,7	0,0	9,7	10,4
	Zahl der Teilnehmer	5.460	1.462	24	142	135	35	144	666

QUELLE: HIMSS; 1 = IN PROZENT ALLER TEILNEHMER, 2 = Q4/2015: 3 = Q4/2016 (ALLE LÄNDER IN DER TABELLE, ZUSÄTZLICH A(14), BE(16), F(13), GR(1), IS(1), IRL(1), N(3), PL(14), P(27), SLO(2), CH(10) UND UK(102)

Digitalisierung in unterschiedlichem Tempo
Wo steht ein Krankenhaus bei der Digitalisierung seiner Patientenakten? Das in den USA entwickelte achtstufige *Electronic Medical Record Adoption Model* (EMRAM) gibt handfeste Anhaltspunkte. Ausgehend von Stufe 0 ist bei Stufe 7 das Optimum erreicht. Die Stufen bauen aufeinander auf, um die Prozesse zu bewerten, die sich wiederum an der Praxis von US-Kliniken orientieren. Wer andere Prioritäten setzt, wie etwa Dänemark, landet im Vergleich hinten. Die Tabelle zeigt, wie viel Prozent der an der HIMSS-Umfrage teilnehmenden Kliniken eines Landes die einzelnen Stufen des Modells bereits digitalisiert haben. [HIMSS = Healthcare Information and Management Systems Society]

Die politische Weichenstellung ist durchaus relevant

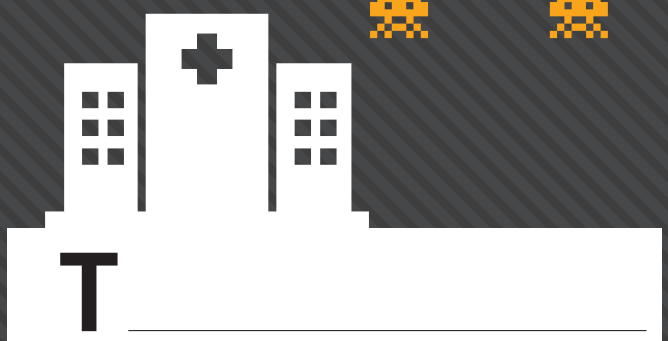
Gesundheitsberater wenden können. Auch in den Krankenhäusern zeichnet sich ein Rennen unterschiedlicher Geschwindigkeiten ab. Als Tachometer dient das achtstufige *Electronic Medical Record Adoption Model* (EMRAM), das die Vollständigkeit elektronischer Patientenakten (EPR) und somit den Grad der Digitalisierung misst. Das Prinzip: Um die nächsthöhere Stufe zu erreichen, müssen die Voraussetzungen der darunterliegenden Stufen erfüllt sein; auf Stufe 7 erreicht ein Krankenhaus die „optimierte klinische operative und Geschäftsprozesseffizienz“. Durch die EMRAM-Brille betrachtet wirken die Unterschiede zwischen den USA und Europa groß. In den USA haben zwei Drittel der Krankenhäuser die drei höchsten Stufen erreicht, in Europa lediglich ein Drittel. Während Deutschland, Frankreich und Großbritannien eher schwach bewertet werden, zeigen Kliniken in Dänemark, Holland, Spanien und der Türkei relativ hohe Bewertungen. In der Türkei? „Ja, eine als eher homogen zu charakterisierende IT-Landschaft innerhalb der Krankenhäuser – mit teilweise sehr ausgereiften Softwarefunktionen – führt zu diesem eindrucksvollen Ergebnis“, erklärt Frank Fritzsche vom EMRAM-Beratungshaus HIMSS.

Die Gründe dafür sind vielfältig. EMRAM wurde in den USA entwickelt und an US-typische Digitalisierungsprozesse angepasst. Außerhalb Amerikas haben viele Kliniken andere Prioritäten gesetzt. So qualifiziert ein digitales radiologisches Bildmanagement eigentlich für die fünfte Stufe; solange ein Krankenhaus die Laborergebnisse aber nicht elektronisch übermittelt, bleibt es auf Stufe 0. Weitere Ursachen finden sich in den nationalen Gesetzgebungen. In Dänemark wurde bereits 1977 ein Patientenregister eingeführt, in den Niederlanden wird die Technisierung des Gesundheitswesens seit den 1980er-Jahren staatlich gefördert, und in Spanien gibt es seit 2008 Pilotprojekte zur Implementierung einer nationalen EPR. Zudem werden öffentliche Krankenhäuser hier nicht auf Grundlage von Patientenzahlen finanziert, sondern auf Basis der Bevölkerungszahl der jeweiligen Region. Mehr Effizienz lässt sich in einem solchen System vor allem durch geringere Kosten, nicht aber durch mehr Umsatz erzielen. Investitionen, auch in die Digitalisierung, folgen einer anderen Strategie. „Die politische Weichenstellung“, betont Fritzsche, „ist ein sehr relevanter Aspekt zur Organisation des Gesundheitssektors.“

Interview:
Was bedeutet es für Krankenhäuser, wenn Informatik und Medizin immer stärker zusammenwachsen?
www.draeger.com/401-10

Wege aus der digitalen Geiselhaft

Die steigende Digitalisierung sorgt in Krankenhäusern für mehr Produktivität und Transparenz. Damit geraten sie allerdings auch ins Visier krimineller Hacker, die mit Ransomware versuchen, die Betreiber zu erpressen: Freischaltung der eigenen Daten nur gegen Zahlung eines Lösegelds! Noch hinken die meisten Sicherheitsstandards dieser Entwicklung hinterher, doch Abhilfe ist möglich.



TeslaCrypt, Locky und Cerber: Diese Erpresser-Programme, die bei Sicherheitsexperten im vergangenen Jahr für die größte Unruhe sorgten, trieben im Frühjahr und in der zweiten Jahreshälfte ihr Unwesen. Die drei Eindringlinge zählen zur Ransomware-Familie, dem neuen Liebling krimineller Hacker. *Ransom* bedeutet Lösegeld, *ware* steht für Software. Dieser digitale Schädling ist ein Spezialist unter den Trojanern. Er dringt in IT-Systeme ein, verschlüsselt geschäftskritische Daten und gibt sie erst nach Zahlung eines Lösegelds wieder frei. 2016 zeigte der Newcomer weltweit, was er kann. Schätzungen zufolge nahm er rund drei Prozent aller Unternehmen in den westlichen Industrieländern in Geiselhaft. US-Firmen waren am häufigsten betroffen, unter den Top 10 der Rangliste fanden sich zudem Länder Europas sowie Kanada, Australien und Indien.

Krankenhäuser ähnlich stark betroffen

Bei Krankenhäusern lag die Quote nach Schätzung von Experten ähnlich hoch wie in anderen Branchen. Weil Betriebsabläufe oft für mehrere Tage gestört waren, zeigten viele Kliniken den Angriff an. Ein Krankenhaus in Los Angeles gab sogar zu, umgerechnet 15.000 Euro gezahlt zu haben, um schnellstmöglich wieder Herr der Lage zu sein. Der Rest hüllte sich in Schweigen, weil eine erfolgreiche Erpressung unweigerlich Nachahmer auf den Plan ruft.

Die Attacken erfolgten nicht gezielt, sondern flächendeckend. Irgendwo, das garantieren die Gesetze der Statistik, findet sich immer ein Einfallstor. Entweder, weil IT-Netzwerke veraltet oder Mitarbeiter nachlässig sind. Krankenhäuser bilden da keine Ausnahme. Dennoch sind Angriffe für diese Branche immer ein besonderes Alarmsignal, hat Florian Grunow, IT-Sicherheitsexperte beim Beratungshaus ERNW in Heidelberg, beobachtet: „Bis zum Zeitpunkt der Ransomware-Attacken glaubten viele Verantwortliche nicht, im Fokus von Hackern zu stehen.“ Der Grund: Patientendaten gelten, im

ILLUSTRATION: PICFOUR

Geld her! Dieser rüde Befehl ist die Kurzfassung dieses Screenshots. Wer ihn erblickt, kann entweder in anonymen Bitcoins zahlen oder zusehen, wie die eingeschleuste Software Datei um Datei löscht. Mit etwas Glück befreit die Lösegeldzahlung die Daten wieder aus der Geiselhaft. Eine Garantie dafür gibt es jedoch nicht. Man kann mit unterschiedlichen Strategien darauf reagieren

Heute lässt sich eine Erpressung komplett automatisieren

Vergleich zu Konstruktionsdaten produzierender Unternehmen, in Deutschland als schwer verkäuflich. Ransomware zielt allerdings nicht auf Datenklau, sondern auf Erpressung. „Dieses Szenario ist auch für Krankenhäuser neu, zudem höchst relevant“, sagt Grunow. „Die meisten Kliniken sind darauf nicht vorbereitet.“ Und es gibt gute Gründe anzunehmen, dass die Bedrohung weiter wächst. So verdienen kriminelle Hacker mit Ransomware wesentlich leichter Geld als mit traditionellen Späh-Programmen. Letztere ziehen viel Arbeit nach sich, weil man erst einmal zahlungskräftige Abnehmer finden muss. Bei Ransomware dagegen wird das Opfer selbst zur Kasse gebeten. Sobald der digitale Schädling ein IT-System unter Kontrolle gebracht hat, steigt die Wahrscheinlichkeit, dass innerhalb kurzer Zeit das Lösegeld fließt. Aufwand und Risiko tendieren für den oder die Erpresser praktisch gen null. Der gesamte Prozess (Einschleusen, Erpressung, Freigabe) lässt sich sogar automatisieren. Zudem ist der Zugang zu Ransomware-Programmen relativ einfach. Im Darknet (dem Teil des Internets, in dem man sich mithilfe moderner Verschlüsselung anonym bewegen kann) stellen „Dienstleister“ individuelle Ransomware quasi aus dem Baukasten zusammen – und ergänzen sie mit nützlichen Zusatzfunktionen, wie eine Übersicht der Zahlungseingänge oder einen technischen Kundendienst. Dafür behalten sie einen Teil der Einnahmen ein, die der Erpresser erlöst.

Angriffsfläche für Ransomware wächst

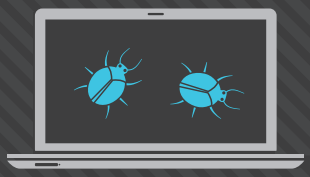
Während ein IT-Netzwerk noch vor wenigen Jahren im Wesentlichen aus PCs, Druckern und Festplatten bestand, sind heute auch Telefonanlagen, Fahrstühle, Videoüberwachung, TV-Monitore oder medizinische Geräte eingebunden. Damit steigt nicht nur die Zahl der benötigten Schnittstellen und die Komplexität der Netzwerke, sondern auch die Wahrscheinlichkeit, dass Programmierfehler in der Software, die Hackern unbemerkt Hintertüren ins IT-System öffnen, ausgenutzt werden. Das größte Risiko aber bleibt der Mensch. Vielen Mitarbeitern sind die Folgen ihres Handelns oft gar nicht bewusst. Die Zahl derjenigen, denen Laptops oder Smartphones gestohlen werden, die arglos E-Mail-Anhänge öffnen, ausgespäht werden oder gar Passwörter preisgeben, wächst mit dem Tempo, mit dem die Digitalisierung Einzug erhält. Regelmäßige Schulungen und eine sensibilisierende Unternehmenskultur gelten als wichtige Säulen einer erfolgversprechenden Sicherheitsarchitektur. Um die technische Infrastruktur auf Herz und Nieren zu prüfen, setzen Spezialisten Methoden ein, die nicht zufällig an Geheimdienste erinnern. Nur wenn die Architektur der Systeme modular aufgebaut ist, lassen sich Schadprogramme schnell isolieren und deren Verbreitung stoppen. Manchmal sind allerdings selbst kritische Bereiche offen wie ein Scheunentor. „Wir haben es bei unserem Test →

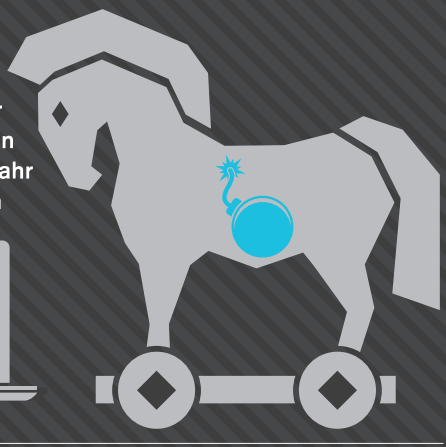
RANSOMWARE – ERPRESSUNG MIT IT

Geiselnahme von Menschen ist ein kriminelles Geschäftsmodell – die von IT-Systemen ebenfalls. Dort verschlüsselt eingeschleuste *Ransomware* die Daten, die nur gegen Zahlung wieder freigeschaltet werden. Einblicke in einen oft versteckten Bereich.

2.896

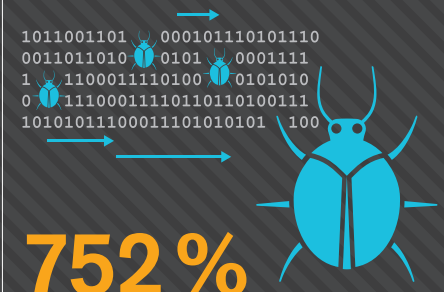
verschiedene Ransomware-Trojaner entdeckten Experten der russischen IT-Sicherheitsfirma Kaspersky im Jahr 2016 allein auf mobilen Computern





4.000

Ransomware-Angriffe gab es 2016 – täglich und allein in den USA. Das ist gegenüber dem Vorjahr eine Steigerung um 300 Prozent

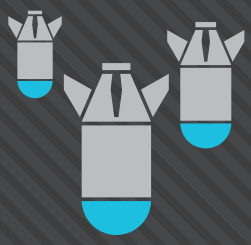


752 %

Steigerung bei der Anzahl der Ransomware-Familien gab es im Jahr 2016 gegenüber 2015

40 %

aller Spam-Anhänge enthielten Ransomware im Durchschnitt des Jahres 2016. Ein Jahr zuvor lag der Prozentsatz dieser Erpressungssoftware bei nur 0,5 Prozent



Um mehr als 1.000 %

stieg die Anzahl der Ransomware-Attacken in Deutschland in der Zeit zwischen Oktober 2015 und Februar 2016. Weltweit wuchs sie um den Faktor 6

30 %

der Angegriffenen erfüllen die Lösegeldforderung, um wieder an ihre Daten zu kommen

50.000

US-$ und mehr würde jedes dritte größere Unternehmen in den USA bezahlen, um nach einer Attacke wieder Zugang zu seinen Geschäftsunterlagen zu erhalten

BILDSCHIRMFOTO: IBM; ILLUSTRATIONEN: PICFOUR; QUELLEN: U.S. DEPARTMENT OF JUSTICE, KASPERSKY LAB, INTERPOL, MALWAREBYTES, BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), IBM

Prüfen nach CIA-Methode

Der Name erinnert an einen US-Geheimdienst, tatsächlich geht es auch bei diesem Cyber-Security-Test um Aufklärung. Allerdings steht das Kürzel nicht für *Central Intelligence Agency*, sondern für *Confidentiality* (Vertraulichkeit), *Integrity* (Integrität) und *Availability* (Verfügbarkeit).

Der CIA-Test prüft die Sicherheit von IT-Systemen systematisch nach folgendem Muster:

- Sichert das System Vertraulichkeit, oder bietet es offene Fenster, durch die sich Daten auf dem Weg zum Empfänger heimlich mitlesen lassen?
- Garantiert es die Integrität der Daten, oder gibt es Schwachstellen, die es Hackern ermöglichen, Daten zu verändern und etwa auf einem Patientenmonitor falsch auszugeben?
- Gewährleistet es höchste Verfügbarkeit, oder bietet es Lücken, die Hacker nutzen können, um das System durch Überlastung oder Verschlüsselung zum Erliegen zu bringen?

Medizingeräte, die sich wie ein Smartphone steuern lassen?

in einem Krankenhaus beispielsweise geschafft, ein MRT über das offene Patienten-WLAN zu übernehmen und auch Spritzenpumpen darüber zu steuern“, sagt Grunow.

Normen helfen beim Risikomanagement

Doch die verbindlichen Maßnahmen zur Gefahrenabwehr mehren sich. 2012 wurde die Norm IEC 80001 novelliert, sie beschreibt das Risikomanagement für den Betrieb von IT-Systemen in Krankenhäusern. 2013 gab das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Leitfaden zum Thema „Risikoanalyse Krankenhaus-IT“ heraus. 2015 verabschiedete der Deutsche Bundestag das IT-Sicherheitsgesetz. Wenig später zog die Europäische Union mit der Richtlinie zur Nationalen IT-Sicherheit (NIS) nach; sie sieht unter anderem den EU-weiten Aufbau von Behörden und Spezialtrupps vor, eine stärkere Zusammenarbeit der Länder sowie verbindliche Meldepflichten. Kürzlich eröffnete die britische Regierung in London das erste National Cyber Security Center. Da sie für die nationale Gesundheitsversorgung eine kritische Rolle spielen, rücken auch Krankenhäuser in den Fokus. Beispiel Deutschland: Das IT-Sicherheitsgesetz dürfte die Infrastruktur der größten Kliniken des Landes als besonders schützenswert definieren. Michael Thoss, Pressereferent des Bundesverbands der Krankenhaus-IT-Leiterinnen/Leiter e.V., erkennt in dieser Entwicklung Herausforderungen und Chancen. „Für die klassischen IT-Bereiche dürfte das Sicherheitsgesetz bis auf die Audits überschaubare Konsequenzen haben, weil das Verantwortungsbewusstsein für personenbezogene Daten hier schon immer stark ausgeprägt war. Dagegen könnten in der Medizintechnik künftige Zertifizierungen sehr viel Aufwand nach sich ziehen.“

Die US-Gesundheitsbehörde FDA hat auf diesen Befund bereits reagiert: Im Oktober 2014 veröffentlichte sie zunächst eine *premarket guidance* und Ende 2016 einen 30-seitigen Leitfaden zum Management von IT-Sicherheitsrisiken bei vernetzten Medizingeräten. Darin werden Hersteller unter anderem aufgefordert, das Thema Cyber-Security nicht nur bei der Entwicklung und Produktion, sondern auch bei der Wartung stärker als bisher zu verfolgen. Im Vordergrund steht für Hersteller die Frage, wie sie auf bekannt gewordene Sicherheitslücken reagieren sollen. Fest steht: Die Steuerung von Beatmungsgeräten, Insulinpumpen oder Dialysemaschinen gleicht sich der von Smartphones immer mehr an. Mit jedem Software-Update werden die Geräte in einen neuen Zustand versetzt. Anders als bei Smartphones wird die Hardware allerdings nicht alle zwei bis drei Jahre ausgetauscht. „Für die Sicherheitsspezialisten in den Krankenhäusern“, sagt IT-Leiter Thoss, „wirft diese Entwicklung ganz neue Fragen und Tätigkeitsfelder auf.“ ◄

Die Kunst des Weglassens

Technik, Normen, Gesetze: Um vernetzte Medizintechnik zu managen, braucht es Experten-Know-how. Dräger schult daher nicht nur Mitarbeiter, sondern auch Kunden.

FOTO: GEORG TROTT

Hannes Molsen
ist für die Datensicherheit aller Produkte bei Dräger verantwortlich

Wer die Strategie des Gegners kennt, kann sich besser vor seinen Angriffen schützen. Die Sicherheitsexperten bei Dräger beschäftigen daher auch einen *Certified Ethical Hacker* (CEH). Er beherrscht das Werkzeug krimineller Hacker, führt aber ausschließlich Gutes im Schilde. Auch Hannes Molsen, Leiter Produktsicherheit bei Dräger, ist ein bekennender Hacker – doch für ihn ist der Begriff viel zu negativ besetzt: „Ursprünglich verstand man darunter die Neugier, technische Systeme für etwas zu gebrauchen, für das sie nicht gedacht waren." Zwei Joghurtbecher, die man mit einem Faden verbindet, um zu telefonieren, zählt er bereits dazu. Das Hacking im Cyberspace sowieso. Molsens Bereich wurde vor drei Jahren geschaffen, kümmert sich um die Sicherheit der Dräger-Produkte und die Frage, wie sich deren digitale Angriffsfläche verringern lässt. Drahtlose Schnittstellen, ob Bluetooth oder WLAN, stehen dabei ebenso auf dem Prüfstand wie Betriebssysteme. Dabei lautet ein wichtiges Leitmotiv: Was nicht wirklich benötigt wird, wird gar nicht erst installiert.

Die zwei Seiten der Sicherheit

Dabei geht es immer um zwei Aspekte der Produktsicherheit: *Safety* und *Security*. Safety fragt, wie sich die Gesundheit des Anwenders vor den Unzulänglichkeiten des Produkts schützen lässt. Und Security verfolgt, wie sich das Produkt vor Missbrauch durch den Anwender schützen lässt. „Wenn etwa funkgestützte Gaswarngeräte durch einen Hackerangriff ausfallen, würde der Betreiber die betroffene Produktionsanlage evakuieren. Dabei käme vermutlich niemand zu Schaden, dem Kunden der Ausfall finanziell jedoch teuer zu stehen." Vernetzung und Mobilität sind wesentliche Treiber der Digitalisierung, auch in der Medizintechnik. Alarme, die verschiedene Geräte von Vitaldaten erzeugen, können noch genauer werden, wenn man sie miteinander vernetzt. Auch die automatisierte Datenübertragung kommt dem Patientenwohl zugute – etwa weil die Gefahr sinkt, Patientendaten und Medikamente zu vertauschen, oder weil man die Vitaldaten von Patienten über einen Monitor auch aus der Ferne im Auge behalten kann. Soweit die Theorie. In der Praxis gilt es, Fehler schnell zu beheben. Nur: Wer ist für einen Ausfall verantwortlich? Das IT-Netzwerk oder die Medizintechnik? Molsen beschreibt die Sicherheitsphilosophie bei Dräger wie folgt: „Die Netzwerke müssen mit unsicheren Endgeräten und die Endgeräte mit unsicheren Netzwerken umgehen können. Dann kann sich keiner den Schwarzen Peter zuschieben." Seit Veröffentlichung der deutschen Fassung der IEC-Norm als DIN EN 80001-1 im Jahr 2011 steht das Risikomanagement vernetzter Medizintechnik auch in vielen Krankenhäusern ganz oben auf der Agenda. Die Norm beschreibt einen Risikomanagementprozess für medizinische IT-Netzwerke, um einen sicheren und störungsfreien Betrieb vernetzter Medizinprodukte zu gewährleisten. Zudem gibt sie mit Safety, Security und Effektivität drei Schutzziele vor, deren Einhaltung der Betreiber mit einem Risikomanagement nachweisen kann. „Daraus ergeben sich zwingend Ansätze der interdisziplinären Zusammenarbeit der Organisationseinheiten Medizintechnik und IT", sagt Jutta Antwi-Schultze-Lebenstedt. Sie leitet die Kundentrainings der Dräger Academy in Deutschland. Im Schulungskatalog findet sich seit 2012 auch der Workshop „DIN EN 80001-1 – Risiken erfolgreich managen" sowie – darauf aufbauend – der Zertifikatslehrgang „Medical-IT-Network-Riskmanagement" (IHK). Er richtet sich an Fach- und Führungskräfte aus den Bereichen Medizintechnik, Informationstechnologie, Qualitäts- und Prozessmanagement sowie Organisationsentwicklung: „Somit unterstützen wir die Anforderungen im Gesundheitswesen als bislang einziges Unternehmen bundesweit, das eine IHK-zertifizierte Ausbildung zum Medical-IT-Network-Riskmanager anbietet." ◄