1 Cybersicherheit als Prozessenabler für Digitalisierung

Hans-Wilhelm Dünn

1.1 Cybersicherheit für Krankenhäuser

Am Morgen des 10. Februar 2016 öffnete eine Mitarbeiterin des Lukaskrankenhauses in Neuss die Anlage einer E-Mail mit „Rechnung“ in der Betreffzeile. Kurze Zeit später gingen bei der IT-Abteilung ungewöhnlich viele Fehlermeldungen ein. Die IT-Infrastruktur wurde durch einen Verschlüsselungstrojaner in die Knie gezwungen, Erpressungsgelder verlangt. Die Klinik fuhr alle ihre Systeme herunter und stellte auf analogen Notbetrieb um: Boten statt digitaler Meldungen, Handbetrieb statt Rechner. Manche Operationen konnten nicht stattfinden und Forensik, Daten-Backup und Krisenmanagement verursachten Kosten von über einer Mio. Euro. Die Schattenseite der Digitalisierung sind Cyberkriminalität und Cyberangriffe. Prozesse werden durch die digitale Transformation vereinfacht und beschleunigt. Das gilt aber eben auch für Prozesse der Kriminalität. Cyberangriffe nehmen zu, entwickeln sich weiter und richten größeren Schaden an.

Angesichts dieser Bedrohungssituation ist Cybersicherheit ein Prozessenabler, eine notwendige Bedingung für die Digitalisierung. Nur durch Cybersicherheit können die Gefahren der Cyberkriminalität abgewehrt und die positiven Effekte der Digitalisierung genutzt werden. Diese Interdependenzmechanismen zwischen Digitalisierung, Cyberkriminalität und Cybersicherheit betreffen Krankenhäuser und die Gesundheitsbranche in extremerer Form, weil Krankenhäuser gleichzeitig attraktiveres und verletzlicheres Target für Cyberkriminelle sind. Zunächst werden in diesem Beitrag die aktuellen Digitalisierungstrends definiert und in den Kontext der globalen Digitalisierung als Großtransformation des späten 20. Jahrhunderts eingeordnet. Anschließend wird der Bogen zwischen disruptiver Digitalisierung und dem Kran-

kenhaus geschlagen. Im Anschluss wird die Bedrohungskulisse von Cyberangriffen und Cyberkriminalität illustriert und wieder genauer auf die spezielle Ausgangslage im Krankenhaus bezogen. Als letzter Schritt wird aufgezeigt, inwiefern Cybersicherheit sowohl für die Digitalisierung im Allgemeinen als auch bei der Digitalisierung im Besonderen – im Krankenhaus – die einzige Möglichkeit ist, die Vorteile der Digitalisierung zu nutzen, ohne sich den Gefahren von Cyberangriffen aussetzen zu müssen.

1.2 Digitalisierung ist disruptiv und transformativ

Pierre Nanterne, der Chief Executive Officer des Consulting Unternehmens Accenture, erklärte in einem Artikel für das World Economic Forum die „Digital Disruption" zu einer zentralen Herausforderung der Gegenwart. Digitale Disruption beschreibt die Verdrängung und Ablösung bestehender Produkte, Dienstleistungen und Unternehmen durch digitale Innovation. Disruptive Innovation sorgt für eine Umstrukturierung der betroffenen Märkte von Grund auf. Nanterne illustriert das disruptive Potenzial digitaler Technologien und Innovationen damit, dass innerhalb der letzten 19 Jahre mehr als die Hälfte der Unternehmen des Fortune 500 Index verschwunden seien. Für Nanterne sind die Triebkräfte und „Zerstörer" dieser neuen Welle die SMAC Technogien (*Social, Mobile, Analytics and Cloud*) für Nutzer und Unternehmen, künstliche Intelligenz und *Cognitive Computing*, Robotik sowie das *Internet of Things* (IoT). Diese Schlüsseltechnologien sind das disruptive Potenzial, dass die Geschwindigkeit und das Potenzial der „vierten industriellen Revolution" ausmachen. Sie ermöglichen das Erschließen neuer Sektoren und Märkte, datenbasierte Verbesserungen bei Qualität und Produktivität und Innovationen in völlig neuen technologischen Sektoren. An der vordersten Front der digitalen Revolutionen steht das disruptive Potenzial als Treiber (Nanterne 2016).

Es zeigt sich in der langfristigen Entwicklung des Fortune 500 aber auch, dass die Digitalisierung ein langwieriger Transformationsprozess ist. Seit 1955 listet Fortune die profitabelsten und wertvollsten amerikanischen Unternehmen nach Profit und Umsatz. Im Jahr 1955 dominierte die Montanindustrie, Automobilfirmen und Ölproduzenten die vorderen Ränge der Fortune 500 mit Namen wie General Motors, Exxon Mobil, U.S. Steel und Chrysler. Im Jahr 2019 sind die profitabelsten Firmen der USA Apple, die Großbank JPMorgan Chase und Googles Mutterkonzern Alphabet. Wo in der ersten Ausgabe der Fortune 500 Stahl, Öl und Autos die meisten Profite brachten, sind jetzt die Tech-Firmen und Finanzdienstleister die vordersten Leistungsträger der amerikanischen Wirtschaft. Der Shift ist in der zweiten Hälfte des 20. Jahrhunderts vollzogen worden, er fällt zusammen mit der technologischen Revolution. Die technologische Revolution ist ein andauernder Umbruch, gekennzeichnet von der Umwandlung analoger in digitale Prozesse. Anfänge und Vorläufer der Digitalisierung sind seit Mitte des 20. Jahrhunderts sichtbar und mit der Jahrtausendwende haben Digitalisierungsprozesse zu einer Umwandlung der Gesellschaft, Wirtschaft, Wissenschaft, Politik und vielen anderen Bereichen geführt. Die jüngste Ausprägung dieses kontinuierlichen disruptiven Umbruchs ist die „vierte industrielle Revolution". Getragen von den Möglichkeiten, analoge in digitale Prozesse umzuwandeln, geht es nunmehr um die Vernetzung von Rechnern, Datenzentren und Geräten sowie die digitale Verarbeitung von Daten (Nanterne 2016; Perry 2017).

1.3 Die „vierte industrielle Revolution“ im Krankenhaus

Es wäre angesichts der Dominanz von Technologieunternehmen zulasten der klassischen Industrie in den oberen Rängen der Fortune 500 falsch, die Digitalisierung rein in der Technologiebranche zu verorten. Die „vierte industrielle Revolution“ zeichnet sich ja gerade dadurch aus, dass die Umwälzungen und das disruptive Potenzial der digitalen Innovation auch in nicht-digitale Branchen und Sektoren getragen werden. Dem Wirtschaftswissenschaftler Klaus Schwab zufolge schließt sich die vierte industrielle Revolution unmittelbar an die technologische Revolution an und steht im Kontext der „klassischen“ industriellen Revolutionen im 18. und 19. Jahrhundert. Die Basis dafür ist ein überall verfügbares und mobiles Internet, leistungsfähige und günstige Sensoren sowie künstliche Intelligenz. Auf dieser Basis aufbauend werden weitere Innovationen ermöglicht, etwa die Sequenzierung von Genen, Nanotechnologie, erneuerbare Energien, Quantencomputer. Der große Unterschied zur ebenfalls schon digitalen „dritten industriellen Revolution“ besteht nach Schwab in der Möglichkeit, interdisziplinär unterschiedliche wissenschaftliche Disziplinen miteinander zu verbinden und, vermittelt durch digitale Technologien, aufzuwerten (Schwab 2016).

Das Potenzial der Digitalisierung der Krankenhäuser ist enorm und schlägt sich auch finanziell nieder. Gemäß einer Studie von McKinsey von Dezember 2018 sind durch Umstellung auf digitale Prozesse Einsparungen von etwa 34 Mrd. Euro aller Gesundheitsausgaben möglich, das entspricht 12% der gesamten Kosten. Der größte Teil dieser Einsparungen, ca. 16,1 Mrd. Euro, entfällt hierbei auf Krankenhäuser und stationäre Aufenthalte in Kliniken. McKinsey sieht Einsparpotenzial durch das Rollout einer Vielzahl von digitalen Lösungen in sechs Lösungskategorien: Umstellung auf Papierlose Daten, Möglichkeiten der Onlineinteraktion zwischen Patienten und Gesundheitsdienstleistern, Ergebnistransparenz und Entscheidungsunterstützung durch Digitale Technik, Automatisierung/Streamlining von Arbeitsabläufen, Möglichkeit der Selbstbehandlung von Patienten sowie Self-Service von Patienten (Hehner et al. 2018).

Innerhalb der Krankenhäuser sehen wir sowohl mikroelektronische Digitalisierung als auch die synergetisch-vernetzte Digitalisierung der „vierten industriellen Revolution“. Wir sehen sowohl die einfache Digitalisierung von analogen Prozessen als auch die beschriebene datengestützte synergetische Aufwertung nicht-digitaler Disziplinen und Techniken. Besonders ist hier natürlich die digitale und vernetzte Medizintechnik zu nennen, die in den nächsten Jahren in allen Krankenhäusern noch mehr und mehr etabliert werden wird. Digitalisierung bedeutet allerdings natürlich auch die nicht primär krankenhausimmanenten Prozesse, die ebenfalls digitalisiert werden. Konkret ist die Digitalisierung in Krankenhäusern eine Umwandlung von analogen und unvernetzten Prozessen zu digital-vernetzen Prozessen.

1.4 Digitalisierung im Krankenhaus

Im Branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) findet sich eine Übersicht über digitale Krankenhausprozesse. Die Deutsche Kran-

kenhausgesellschaft e.V. hat den Standard für den Teil der Krankenhäuser, der unter die Definition des BSI einer Kritischen Infrastruktur fällt (30.000 vollstationäre Fälle im Jahr) vorgesehen. Der B3S ist aber ausdrücklich auch für alle anderen Krankenhäuser empfohlen, die trotz geringerer Fallzahlen und ohne den Titel einer „kritischen Infrastruktur" dem gleichen Angriffspotenzial ausgesetzt sind. Der B3S gruppiert die Prozesse im Krankenhaus in fünf Gruppen, die unterschiedlichen Tätigkeitsbereichen entsprechen. Die Kernprozesse sind in die Bereiche Aufnahme, Diagnose, Therapie, Pflege und Entlassung geordnet und beschreiben die Kernaufgaben der Patientenversorgung (Deutsche Krankenhaus Gesellschaft 2019).

Neben diesen „Kernprozessen" nennt das B3S auch Unterstützungsprozesse, die die Kernprozesse ermöglichen und personell, materiell, logistisch und organisatorisch stützen. Die Unterstützungsprozesse im Krankenhaus umfassen grob die Infrastruktur, das Personalwesen, die Verwaltung, Buchhaltung und Finanzierung und die IT-Infrastruktur des Krankenhauses. Für den B3S bilden hier die Prozesse der Informationstechnik die Basis. Die Kommunikationstechnik umfasst Rufsysteme, Telefonie, Fax-Systeme und hat große und sich vergrößernde Überschneidungen mit der IT. Medizintechnische Geräte bilden einen weiteren großen Bereich. Auch hier ergibt sich wegen der zunehmenden Verschränkung mit der IT eine Zunahme des Digitalisierungsgrades. Die Versorgungstechnik umfasst infrastrukturelle Systeme, Gebäudeleittechnik, Versorgung (Strom, Wasser, Gas, Wärme, Klimatisierung, Be- und Entlüftung) und Entsorgung, Transport und Gebäudeinstandhaltung. Auch hier sind zunehmend Digitalisierungs- und Vernetzungsprozesse zu beobachten, sodass auch hier sowohl synergetische Effizienzgewinne als auch Verletzlichkeitszunahmen zu beobachten sind. Die meisten bisherigen Cyberangriffe auf Krankenhäuser haben nur die IT betroffen (Deutsche Krankenhaus Gesellschaft 2019).

In jedem Krankenhaus laufen täglich hunderte von Prozessen ab. Der Grad der Digitalisierung des Krankenhauses hängt erstens davon ab, wie viele dieser Prozesse von Rechnern übernommen und/oder unterstützt werden und wie viele dieser digitalen Prozesse darüber hinaus mit dem Internet verbunden sind. Deutschland hinkt bei der Digitalisierung seiner Krankenhäuser dem europäischen Durchschnitt hinterher. Das *Electronic Medical Records Adoption Model (EMRAM) der Healthcare Information and Management Systems Society* (HIMSS), einer US-Amerikanischen Non-Profit-Organisation unter anderem zur Verbesserung der informationstechnischen Infrastruktur in Kliniken, misst den Digitalisierungsgrad von Krankenhäusern und stuft Kliniken in acht Stufen ein, je nachdem wie viele ihrer Prozesse digitalisiert sind. Die beschriebenen Digitalisierungsgrade reichen von einzelnen digital arbeitenden Unterabteilungen (Labor, Radiologie und Apotheke, Stufe I), über elektronische Arzneimittelverordnung (Stufe 4) bis hin zu einem mehr oder weniger ungebrochenen digitalen Datenfluss in allen Bereichen und einer ineinandergreifenden IT-Unterstützungsstruktur (Stufen 6 und 7).

Ab den höchsten Stufen werden die Synergieeffekte und Effizienzgewinne der Digitalisierung voll ausgeschöpft. Kliniken der beiden höchsten Stufen, der „Stage 6 and 7 Club", werden durch die HIMSS gesondert ausgezeichnet. Im Krankenhausreport 2019 wurde anhand deren Einstufung im EMRAM der durchschnittliche Digitalisierungsgrad deutscher Krankenhäuser gemessen. Durchschnittlich erreichen deutsche Krankenhäuser – basierend auf den 147 Krankenhäusern, die sich bis 2017 durch die HIMSS haben zertifizieren lassen – hier einen Wert von 2,3. Deutschland liegt hier

klar unter dem europäischen Durchschnitt von 3,6. 40% der bewerteten deutschen Krankenhäuser etwa arbeiten noch völlig analog, während in Ländern wie Spanien, UK und der Türkei kaum ein Krankenhaus und in den Niederlanden gar keine Klinik mit EMRAM Stufe 0 bewertet ist (Stephani et al. 2019).

1.5 Cyberkriminalität und Cybersicherheit

Zum 01.01.2018 hat HIMSS die EMRAM-Kriterien verändert und strengere Cybersicherheitskriterien in seinem Rating etabliert. Damit wird der untrennbaren Verbindung zwischen Digitalisierung und Cybersicherheit Rechnung getragen. Denn: Durch Digitalisierung werden Menschen, Rechner, Datenzentren und Geräte miteinander vernetzt. Innerhalb von Organisationen können Prozesse durch den freien Fluss und die Auswertung von Daten schneller, effizienter und präziser werden. Die Vernetzung gilt aber nicht nur für die internen Nutzer. Systeme, die mit dem Internet verbunden sind, sind gegenüber Angriffen verletzlich.

Das Bedrohungspotenzial durch Cyberangriffe ist enorm und steigt durch die fortschreitende Digitalisierung und die Professionalisierung der Angriffe stetig. Das finanzielle Schadenspotenzial durch Cyberkriminalität liegt, auf die Jahre 2019–2023 gerechnet, bei mehr als 5,2 Billionen US-Dollar weltweit. In den letzten fünf Jahren seit 2019 haben Angriffe um 67% zugenommen. Neben der quantitativen Zunahme der Angriffe und des Schadenspotenzials verändert sich die Cyberkriminalität auch qualitativ: Datendiebstahl ist zwar immer noch das Hauptziel, aber auch Kernsysteme wie industrielle Leittechnik wird zunehmend zum Zwecke der Störung und Zerstörung gehackt.

Auch bei Daten als Ziel ist der Diebstahl oder die Löschung der Daten nicht mehr die ausschließliche Taktik. Das Verändern von Daten und damit der Eingriff in deren Integrität ist eine neue Dimension der Cyberangriffe. Zu den Veränderungen bei Zielen und Taktiken kommen veränderte Techniken. Vielfach wird durch die neueste Generation von Angriffen nicht mehr das technische Layer, sondern der Mensch gehackt. Der *Human Factor* ist bei der Cybersicherheit das schwächste Glied in der Kette. Auf Deutschland bezogen ergibt sich ein ähnliches Bedrohungspotenzial. Dem Lagebericht des BSI über die IT-Sicherheit zufolge liegt der Schwerpunkt der Bedrohung bei der Cyberkriminalität, durch Malware und Ransomware. Cyberangriffe, generell, nehmen global zu, ihre Technik wird raffinierter und ihr Schaden wird größer (Bissell et al. 2019; Bundesamt für Sicherheit in der Informationstechnik 2019).

Was für Unternehmen generell gilt, gilt in Krankenhäusern in verschärfter Form. Die IT von Krankenhäusern ist gegenüber Cyberangriffen aus unterschiedlichen Gründen besonders verletzlich. Darüber hinaus gehen die potenziellen Schäden von Angriffen weit über die in anderen Institutionen hinaus. Außerdem können Krankenhäuser sowohl in der Prävention als auch in der Abwehr und Nachsorge von Cyberangriffen auf weniger Ressourcen und einen kleineren Werkzeugkasten zurückgreifen.

Im Vergleich zu einem herkömmlichen Unternehmen muss jedes Krankenhaus hunderte von Prozessen in seinen Kern- und Unterstützungsprozessen organisieren und schützen. Diese Prozesse sind in den heutigen Krankenhäusern teils digital gelöst,

teils noch analog. Durch die Digitalisierung als fortschreitender Prozess innerhalb laufender organisatorischer Abläufe sind die digitalisierten Prozesse in den meisten Krankenhäusern nicht zentral designt und innerhalb einer ganzheitlichen Infrastruktur organisiert, sondern sind über die Jahre und je nach Budgetsituation organisch gewachsen. So ergibt sich eine kaum zu überblickende Vielfalt miteinander mehr oder weniger verbundener heterogener Prozessen. Hinzu kommt, dass teilweise nicht aktuelle Hard- und Software verwendet wird, die instabil oder nur langsam funktioniert. Durch veraltete, miteinander vernetzte Technik wird jedes Gerät zum möglichen Einfallstor (Stephani et al. 2019).

Während die Vielfalt der Prozesse durchaus in anderen Organisationen auch auftreten könnte, gibt es bei der Prioritätensetzung und dem Schadenspotenzial im Krankenhaus ein Alleinstellungsmerkmal. Für Unternehmen ist Profitstreben ein Grund, Prozesse zu digitalisieren und diese auch abzusichern. Für Krankenhäuser geht es nicht nur um Profite, sondern auch um das Wohl von Patienten. Die Schäden eines potenziellen Cyberangriffes sind im Krankenhaus nicht nur finanziell. Es kann im schlimmsten Fall um Leben und Tod von Patienten gehen, was in die Risikokalkulation einfließen muss. Bislang ist es zu keinem Angriff gekommen, wo Menschen zu Schaden gekommen sind. Die bisher erfolgten Angriffe auf Krankenhäuser in Deutschland (etwa Neuss im Jahr 2016 oder die DRK Trägergesellschaft Süd-West im Juli 2019) sind in dieser Hinsicht glimpflich verlaufen, weil nur die IT betroffen wurde und das Krankenhaus analog weiterarbeiten konnte. Medizinische Geräte in der OP und Gebäudetechnik sind bisher nicht betroffen gewesen. Das Bedrohungspotenzial steigt aber auch hier durch Vernetzung von Prozessen und Geräten: Angreifer könnten sich theoretisch in Medizintechnik einhacken und Werte anpassen oder Medikationen verändern, wenn die Geräte mit dem Internet verbunden und ungeschützt sind. Neben der Medizintechnik ist auch die Gebäudeleittechnik ein mögliches Risiko. Bei Angriffen auf die Stromversorgung und Ausfällen in der Intensivstation, im OP oder anderen kritischen Stellen können Menschenlebeben gefährdet werden (Wehrs 2019).

Die schwierige Ausgangslage durch die Vielfalt der Prozesse und das fatale Schadenspotenzial sollte eigentlich zu einer Priorisierung von Cybersicherheit in den Kliniken führen. Trotzdem fehlen in deutschen Krankenhäusern ausreichende Budgets für die IT und die IT-Sicherheit. Ein Grundproblem ist hier das Prinzip der „dualen Finanzierung" von Krankenhäusern. Die laufenden Kosten des Krankenhauses werden von den Krankenkassen, die Investitionskosten aber von den Bundesländern getragen werden. Dem GKV-Spitzenverband, Verband der Privaten Krankenversicherung und der Deutschen Krankenhausgesellschaft (DKG) zufolge liegt der bestandserhaltende Investitionsbedarf deutscher Krankenhäuser bei 6 Mrd. Euro im Jahr, um Ausstattung und Infrastruktur zu erhalten. Von den Bundesländern wird davon allerdings nur die Hälfte getragen. Für eine Investition in Cybersicherheit fehlen die Mittel, zumal die Ausgaben für die IT keine hohe Priorität für die Krankenhäuser haben: Deutsche Krankenhäuser geben ca. 1,5% ihres Budgets für die IT aus, Kliniken in den Niederlanden, der Schweiz und Österreich hingegen durchschnittlich 4%. Dem Bundesverband der Krankenhaus-IT Leiterinnen und Leiter e.V. zufolge fehlen den IT-Abteilungen der deutschen Krankenhäuser insgesamt 12 Mrd. Euro. Zur finanziellen Unterversorgung kommt der personelle Fachkräftemangel sowohl bei Medizininformatikern als auch bei IT-Sicherheitsfachkräften. Zusammengefasst: eine schwierige

Ausgangslage mit großem Schadenspotenzial kann wegen einer schwierigen Ressourcenlage schwer verbessert werden (DKG et al. 2019; von Eiff u. von Eiff 2017; o.N. 2018).

1.6 Cybersicherheit ist notwendige Bedingung für Digitalisierung

Der Ist-Zustand der deutschen Krankenhäuser ist ein Digitalisierungs-Limbo. Die Kliniken hängen zwischen einer völlig analogen (und damit cybersicheren, aber nicht zukunftsfähigen) Arbeitsweise und einer digitalen, aber ganzheitlich aufgesetzten und abgesicherten Arbeitsweise fest. Es kann nur in eine Richtung gehen, ein Festhalten an analogen Prozessen ist keine Alternative. Notwendig vernetzte Medizin- und Unterstützungstechnik und eine Erwartungshaltung von Patienten und Gesundheitsdienstleistern wird die Krankenhäuser dazu zwingen, sich erstens zu digitalisieren und diese Digitalisierung auch abzusichern.

Die Schwierigkeit liegt hier in der speziellen Ausgangslage des Krankenhauses, in dem Cybersicherheit organisatorisch und systemisch äußerst schwierig herzustellen und aufrechtzuerhalten ist. Eine Vielzahl von Prozessen bedeuten eine Vielzahl von Einfallstoren, und jeder digitalisierter Prozess stellt eine weiter Öffnung dar, durch die Cyberangriffe ausgeübt werden können. Datenverluste bei Patientendaten betreffen sehr viel intimere Informationen als herkömmliche Datenleaks und bei einem Cyberangriff auf ein Krankenhaus sind die Risiken höher und die potenziellen Schäden größer, da im schlimmsten Fall Menschenleben auf dem Spiel stehen können. Diese suboptimale Situation wird durch die Weiterentwicklung der Digitalisierung noch verschärft: Immer mehr Krankenhausprozesse werden digitalisiert und damit zum möglichen Angriffsziel. Ohne Cybersicherheit werden die positiven Synergie- und Beschleunigungseffekte digitaler Prozesse durch die negativen Folgen von Cyberangriffen und Cyberkriminalität negiert.

Eine Lösung des Dilemmas verlangt ein ganzheitliches Umdenken auf allen Ebenen, und ein Bewusstsein für Cybersicherheit als ein essenzieller Bestandteil des Risikomanagements im Krankenhaus. Cybersicherheit muss als zentraler Prozessenabler erkannt werden, von dem alle anderen Prozesse abhängen. Auf allen Ebenen des Gesundheitswesens, bei der Leitung der Kliniken bis in der Politik muss ein Paradigmenwechsel stattfinden. Ein Bewusstsein für Cybersicherheit muss aber natürlich auch bei den Mitarbeitenden und Gesundheitsdienstleistern in den Krankenhäusern geschaffen und gestärkt werden. Krankenhäuser müssen ihre Prozesse von Grund auf überprüfen und im Hinblick auf Cybersicherheit anpassen. Prozesse und Strukturen müssen re-designt werden. Der erste und wichtigste Schritt ist ein (Wieder)-Gewinn von Übersicht und Kontrolle über die eigenen Systeme. Welche Netzwerke existieren und wo gibt es Verbindungen nach außen? Es braucht eine Bestandsaufnahme über alle laufenden Prozesse. Darüber hinaus müssen alle Mitarbeitenden für Cybersicherheit sensibilisiert und ihr Verhalten dementsprechend angepasst werden, um Einfallstore zu schließen. Auf allen Ebenen muss Cybersicherheit zu einer Priorität werden, gerade weil die IT-Systeme alles im Krankenhaus verbinden und die potenziellen Schäden deswegen so groß sind.

Diese Re-Priorisierung kann natürlich nur dann funktionieren, wenn sie finanziell unterfüttert und ideell gestützt wird. Eine genügende Budgetierung einer ganzheit-

lichen Cybersicherheitsstrategie erfordert eine gesteigerte Awareness der Geschäftsleitung und des Aufsichtsrates den Problemen der Cybersicherheit gegenüber. Bei der Verteilung von Geldern muss mehr in IT und in ihre Sicherheit investiert werden, nicht nur auf technischer, sondern auch auf menschlicher Ebene. Der Weg zu einer erfolgreichen Cybersicherheitsstrategie erfordert aber auch staatliche Unterstützung, sowohl auf gesetzgeberischer als auch auf finanzieller Ebene. Da nach dem Prinzip der „dualen Finanzierung" die laufenden Kosten des Krankenhauses von den Krankenkassen, die Investitionskosten von den Bundesländern getragen werden, muss auch in den Landesgesundheitsministerien und Staatskanzleien ein Umdenken stattfinden, um Krankenhäuser bei dieser transformativen Großaufgabe zu unterstützen.

Literatur

Bissell K, Lasalle RM, Dal Cin P (2019) The Cost of Cybercrime. Ninth Annual Cost of Cybercrime Study. URL: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 (abgerufen am 03. Februar 2020)

Bundesamt für Sicherheit in der Informationstechnik (2019) Die Lage der IT-Sicherheit in Deutschland 2019

Deutsche Krankenhaus Gesellschaft (2019) Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus. Gesamtdokument

DKG, PKV, GKV (2019) GEMEINSAME PRESSEMITTEILUNG Investitionsbedarf der Krankenhäuser: Aktuelle Auswertung bestätigt Unterfinanzierung durch die Bundesländer. Stand: 21. März 2019. URL: https://www.pkv.de/presse/pressemitteilungen/2019/0321-investitionsbedarf-krankenhaeuser/ (abgerufen am 18. Dezember 2019)

Eiff MC von, Eiff W von (2017) Perspektiven des IT-Managements im Gesundheitswesen. In: Müller-Mielitz S, Lux T (Hrsg.) E-Health-Ökonomie, 71–95. Springer Fachmedien Wiesbaden

Hehner S et al. (2018) Digitalisierung in deutschen Krankenhäusern. Eine Chance mit Milliardenpotenzial für das Gesundheitssystem Düsseldorf/Köln/Frankfurt/Berlin/Wien

Klauber J, Geraedts M, Friedrich J, Wasem J (Hrsg.) (2019) Krankenhaus-Report 2019: Das digitale Krankenhaus. Springer Berlin Heidelberg Berlin, Heidelberg

Müller-Mielitz S, Lux T (Hrsg.) (2017) E-Health-Ökonomie. Springer Fachmedien Wiesbaden

Nanterne P (2016) Digital disruption has only just begun. Stand: 17. Januar 2016. URL: https://www.weforum.org/agenda/2016/01/digital-disruption-has-only-just-begun/ (abgerufen am 21. November 2019)

o.N. (2018) IT-Abteilungen fehlen Milliarden. In: Medizin und Elektronik. Stand: 13. September 2018. URL: https://www.medizin-und-elektronik.de/sonstige/artikel/157679/ (abgerufen am 30. Januar 2020)

Perry MJ (2017) Fortune 500 firms 1955 v. 2017. Only 60 remain, thanks to the creative destruction that fuels economic prosperity. Stand: 20. Oktober 2017. URL: https://www.aei.org/carpe-diem/fortune-500-firms-1955-v-2017-only-12-remain-thanks-to-the-creative-destruction-that-fuels-economic-prosperity/ (abgerufen am 22. November 2019)

Schumpeter JA (2006) Capitalism, Socialism and Democracy, 6. Aufl. Routledge; Taylor & Francis Group [distributor] New York Florence

Schwab K (2017) The fourth industrial revolution. Portfolio Penguin London, UK u.a.

Stephani V, Busse R, Geissler A (2019) Benchmarking der Krankenhaus-IT: Deutschland im internationalen Vergleich. In: Klauber J, Geraedts M, Friedrich J, Wasem J (Hrsg.) Krankenhaus-Report 2019: Das digitale Krankenhaus, 17–32. Springer Berlin Heidelberg

Wehrs H (2019) Praxisleitfaden IT-Sicherheit im Krankenhaus. Antares Computer Verlag GmbH Dietzenbach

Hans-Wilhelm Dünn

Hans-Wilhelm Dünn legte sein Studium an der Universität Potsdam als Diplom-Verwaltungswissenschaftler ab. Von 2007 bis 2009 war er Persönlicher Referent im Büro des Wirtschaftsministers und stellvertretenden Ministerpräsidenten des Landes Brandenburg, den er dort auch bei seiner Arbeit als Beiratsvorsitzender der Bundesnetzagentur unterstützte. Von 2009 bis 2010 war er Mitglied im Aufsichtsrat der Energie und Wasser Potsdam GmbH. Von 2010 bis 2012 war Dünn Geschäftsführer von Security and Safety made in Berlin-Brandenburg e.V. Außerdem war er von 2011 bis 2014 Mitglied im Aufsichtsrat der VIP Verkehrsbetrieb Potsdam GmbH. Er ist aktuell Mitglied im Aufsichtsrat der Klinikum Ernst von Bergmann gGmbH. Als Gründungsmitglied und Präsident – zuvor Vizepräsident und Generalsekretär – des Cyber-Sicherheitsrat Deutschland e.V. (CSRD) ist er unter anderem Leiter des Energy Hubs und berät Betreiber kritischer Infrastrukturen zu cybersicherheitsrelevanten Themen. Er wirkt zudem als Direktor am Aufbau des Forschungsinstituts für Cybersicherheit an der Berlin University of Digital Sciences mit. Sein Fachwissen vermittelt er auf hochrangigen Veranstaltungen und ist häufiger Ansprechpartner für TV-Sender und Gastautor für verschiedene Zeitungen, Fachzeitschriften und wissenschaftliche Publikationen wie das Jahrbuch für Europäische Integration.