STUDIENARBEIT

Hochschule für angewandte Wissenschaften

Technische Hochschule Deggendorf

Fakultät Angewandte Informatik

Technikethische Betrachtung der Digitalisierung im deutschen Krankenhaus seit 2015 bezüglich IT-Sicherheit

Studienarbeit im [...] zum Modul [...]

von:

data

about

me

:)

Prüfer:

awesome guy one

awesome guy two

Deggendorf, 18. Februar 2022

Zusammenfassung

Digitalisierung verändert in Krankenhäusern viele Abläufe und Bereiche. Sie bietet enormes Potenzial für Verbesserungen. Deutsche Krankenhäuser sind vergleichsweise wenig digitalisiert.

Dabei entstehen neue Gefahren und Risiken. Die führen zu schweren IT-Angriffen. Angriffe behindern den Betriebsablauf und richten großen Schaden an. Sie betreffen die Patientensicherheit aller Patienten. Viele Patienten leiden unter Ausfällen. Fundamentale Schutzziele der Informationssicherheit sind bedroht. IT-Sicherheit ist ein Teil von Patientensicherheit.

Mittels einer systematischen und pragmatischen Literaturrecherche in OPAC Deggendorf und Google Scholar wurde untersucht, ob eine verantwortungsvolle Digitalisierung deutscher Krankenhäuser erreichbar ist. Begrenzt wurde die Recherche auf den Aspekt IT-Sicherheit, der Situation in Deutschland und auf den Zeitraum von 2015 bis zur Gegenwart. Mit der Methode wurde keine Arbeit gefunden, welche die formulierte These beantwortet. Also technikethisch betrachtet, ob die deutsche Krankenhausdigitalisierung bezüglich IT-Sicherheit moralisch vertretbar ist. Neu am Beitrag ist diese Untersuchung zur Beantwortung der These für den Zeitraum ab 2015.

Es konnten keine Daten zur IT-Sicherheitsausgabenhöhe oder IT-Fachkräfte-Anzahl von Kliniken gefunden werden. Vorteilhaft ist, dass sich Effizienz, Behandlung, Diagnostik etc. verbessern lassen. Es sind viele Innovationen integrierbar, um Abläufe zu erweitern. Digitalisierung kann als ein wichtiges Mittel zum Fortschritt und zur Entwicklung angesehen werden. Doch sie kostet viel Geld. Neben dem Problem des existierenden Fachkräftemangels kann sie auch Innovationen hemmen und Produktivität verringern. Man kann die IT-Sicherheit erhöhen durch die Verwendung von modernen Programmen und Geräten und aus den Erfahrungen fortgeschrittenerer Länder lernen. Gesetzliche Regulationen erweisen sich als wirkungsvolle Mittel die IT-Sicherheit zu verbessern. Hier muss der Staat, als Verantwortlicher, aktiv sein. IT-Kriminalität verursacht große Schäden. Kriminelle können ganze Klinikverbünde attackieren. Durch stärkere Vernetzung bei Medizingeräten entsteht mehr Angriffsfläche. Im Vergleich zu Unternehmen sind Krankenhäuser viel offener für Besucher und damit anfälliger für IT-Attacken. Meistens basiert ein erfolgreicher Angriff auf Fehlern in der Konfiguration oder der Benutzung von Programmen oder Geräten, wegen inadäquaten Schulungen oder komplizierten Designs. Folgen eines erfolgreichen Angriffs sind finanziellen Schäden, Arbeitsausfälle, Reputationsschäden oder gesundheitliche Verschlechterungen bei Patienten. Der Einsatz von manchen Technologien kann den Patientenschutz erhöhen und verringern. Da die Gefahren und Risiken schwerwiegend sind, ist ein Risikomanagement fundamental wichtig. Zur Erhöhung der IT-Sicherheit trat 2015 in Deutschland das IT-Sicherheitsgesetz in Kraft für „Kritischen Infrastrukturen“, also auch Krankenhäuser. Sie müssen höhere IT-Sicherheitsstandards erfüllen und bestimmte Vorfälle melden. Eine kontinuierliche Zusammenarbeit zwischen Produzenten, Betreibern und Endanwendern ist nötig, um die Patien-

tensicherheit zu erhöhen. Ein Grundvertrauen in Entscheidungsträger und Lösungen fehlt bei vielen Bürgern. In der Zukunft werden mehrere Milliarden Euro in IT-Sicherheit, Notfallkapazitäten und Digitalisierung investiert. Es gibt höhere Strafen für IT-Angriffe auf Krankenhäuser. Bessere Messmethoden wurden entwickelt, z.B. zur Analyse der IT-Sicherheit.

Der IT-Sicherheits-Fachkräftemangel ist ein ernsthaftes Hindernis für die Verbesserung der Situation. Eine Besserung bei der Benutzung ist nötig, da sie eines der größten Probleme darstellt. Auch die Hersteller und Betreiber sind hier gefragt. Das Anwendungs-Design sollte möglichst intuitiv sein. Die Kommunikation mit dem Personal muss stark sein. Gute, praxisnahe Schulungen helfen dabei, Wissen langfristig zu vermitteln. Wenn man die gesetzlich vorgeschriebene IT-Sicherheit umsetzt, dann minimiert man Risiken. Mit dieser Minimierung wird man seiner Verantwortung gerecht.

Abstract

Digitization as a megatrend affects and changes German hospitals significantly. Because of several damaging cyber attacks on hospitals, there is a growing concern about the cyber security of them. The consequences of an attack may vary. In a lot of cases operating failure to some extend is only part of the immediate problems that arise. Taking out the accident and emergency department for example can have disastrous consequences on a patient in dire need of urgent admission to a hospital for (advanced) medical attention. Besides medical, technical and economic consequences, attacks can tarnish the reputation of the attacked hospital and cause a loss of trust in the health system as a whole.

The author conducted a systematic and pragmatic literature search using OPAC Deggendorf and Google Scholar so as to examine the morality of the hospital digitization in Germany since 2015. The search was limited to publications regarding ethics of technology, cyber security in German hospitals and German hospital digitization. New in this essay is a contemplation in regards to cyber security.

The literature found showed a tremendous potential hospital digitization has for patients and hospitals alike. But also changes work routines for the worse (partially), for example by increasing the amount of crucial policies. On one hand, digitization can introduce grave dangers to a hospital. On the other, one is able to mitigate the emerging risks by means of cyber security. Digitization can increase and decrease patient safety at the same time.

These results indicate that hospital digitization includes the moral imperative to secure the IT.

Inhaltsverzeichnis

1 Einleitung und thematischer Kontext

Digitalisierung verändert viele Bereiche und Branchen, auch Krankenhäuser. Sie meint den Einsatz von Informationsverarbeitung durch Computer zur Speicherung, Verbreitung und Nutzung von Daten [vgl. 18, S. 132]. Die Krankenhausdigitalisierung bietet ein großes Potenzial für Innovations- und Produktivitätssteigerung [vgl. 14, S. 49]. Krankenhäuser sind und bleiben ein wichtiger Bestandteil im deutschen Gesundheitssystem [vgl. 15, S. 55]. Doch deutsche Krankenhäuser sind wenig digitalisiert [vgl. 18, S. 132].

Die ähnlichen Begriffe IT-Sicherheit und Cyber Security und Informationssicherheit (auf IT bezogen), Krankenhaus und Klinik, IT-Angriff und IT-Attacke etc. werden im Essay synonym verwendet, das heißt es wird zwischen ihnen nicht unterschieden.

„Ethische Diskussionen stehen hoch im Kurs“ [17, S. 16]. Der Trend aus den 70er-Jahren setzt sich fort, die Bedeutung von Ethik rückt immer mehr in den Fokus der Gesellschaft [vgl. 17, S. 16]. Moralische Komplikationen bei Themen wie Ökologie, Globalisierung oder Atomenergie haben nicht an Aktualität oder Relevanz verloren und werden weiter in der Öffentlichkeit diskutiert [vgl. 17, S. 16]. Obwohl diese Beobachtungen ca. 12 Jahre alt sind, kann man, z.B. an aktuellen Klimawandeldiskussionen, Thematiken zu entstehenden Lieferkettenengpässen oder immer neuen Debatten zur Atomenergie, auch für die Gegenwart ihre Gültigkeit bezeugen. Folgen von der Entwicklung sind z.B. Ethikkommissionen in Krankenhäusern und die weitere Entwicklung der spezielleren Wissenschaftsdisziplin Technikethik [vgl. 17, S. 16].

Technikethik ist ein auf gesellschaftliche Nachfrage reagierendes, problemorientiertes, angewandtes Ethikfeld, welches Innovationen und Ideen ethisch beurteilt und Folgen für zukünftige Entscheidungen entwickelt [vgl. 4, S. 5]. Dazu braucht es eine Zusammenarbeit zwischen Technikwissenschaften, Sozialwissenschaften und Philosophie [vgl. 4, S. 5f.]. Gründe für Auseinandersetzungen sind unterschiedliche Vorstellungen von Zukunft, Mensch und Gesellschaft [vgl. 4, S. 5]. Bei der ethischen Reflexion des gegenwärtigen Stands und der Folgen ist eine Betrachtung alternativer Optionen wichtig [vgl. 4, S. 5]. Nachfrage kommt z.B. von Politik, Wissenschaft, Herstellern oder Öffentlichkeit, an die Ergebnisse geliefert werden. [vgl. 4, S. 5]. Leitfragen können sein: Sollte eine Technik gefördert oder reguliert werden, oder was gilt für deren Einsatz? [vgl. 4, S. 5]. Grundsätzliche Fragen zur Beziehung von Mensch, Natur und Technik verlassen angewandte Ethik [vgl. 4, S. 6].

1.1 Problemstellung

Das Gesundheitswesen (allgemein) ist für IT-Kriminelle viel attraktiver geworden [vgl. 5, S. 49]. Das Risiko ist so groß wie noch nie zuvor [vgl. 11, S. 1]. Die Angriffstechniken verbessern sich fortlaufend [vgl. 5, S. 50]. 2016 allein sind ca.

100 Krankenhäuser in Deutschland durch einen IT-Angriff attackiert worden [vgl. 13, S. 53]. Folgen für den Klinikbetrieb sind Terminabsagen, Operationsausfälle, Verschiebung von dringenden Untersuchungen etc. [vgl. 11, S. 1]. Es lassen sich hochsensible Gesundheitsdaten abgreifen (z.B. für späteren Verkauf), sowie kann durch Verschlüsselung der Daten oder Veröffentlichungsdrohung Geld erpresst werden [vgl. 5, S. 49f.]. Dies kann den Betriebsablauf stark bis vollständig aufhalten. Der vollständige IT-Ausfall in einem Krankenhaus verursacht einen schnellen Behandlungskapazitätsverlust [vgl. 23, S. 445]. In vielen Krankenhäusern hat die IT-Sicherheit Mängel [vgl. 3, S. 23]. Gründe dafür sind vielfältig. Beispielsweise kann bei den Verantwortlichen eine unrealistische Grundeinstellung bzgl. angeblicher Ohnmacht gegenüber Angriffen existieren [vgl. 5, S. 49].

Die „Gefahr für deutsche Kliniken steigt“ [13, S. 53]. Aber in der Branche gibt es für die IT (und IT-Sicherheit speziell) nur ein kleines Budget [vgl. 5, S. 49]. Ist dies verantwortungsbewusst?

1.2 Ziele

Das Essay soll am Anfang, in 1, einen Kontext liefern, welcher die aktuelle Situation (und Problematik) aufzeigt und dabei kurz auf Krankenhäuser und Technikethik eingeht sowie Herausforderungen und These erläutert. Danach in 2 die Methodik beschreiben, die Ergebnisse in 3 geordnet präsentieren und beurteilen sowie abschließend in 4 ein Fazit ziehen. Ziel der Arbeit ist es, mit dem in 2 beschriebenen Vorgehen, herauszufinden, ob Krankenhäuser ihrer Verantwortung (zum Schutz von Leben und Privatsphäre) gerecht werden und zu einer Entscheidung bzgl. der These (1.4) zu kommen. Die Arbeit soll die Relevanz des Themas verdeutlichen, es ethisch betrachten, leicht verständlich sein, wissenschaftliche Standards einhalten und Informationen aus überwiegend wissenschaftlichen Quellen nutzen.

1.3 Herausforderung

Die Management-Herausforderung ist Digitalisierung und Vernetzung bei kleinem Budget und Sicherstellung von verantwortungsvoller Datennutzung voranzubringen [vgl. 14, S. 50]. Die in 1.1 angesprochenen Defizite lassen sich nur teilweise durch Erhöhung von Budgets oder Investitionen bewältigen. Es braucht z.B. auch Zeit, Gesetze mit Vorgaben sowie Strafen und die Kompetenzen/Fachkräfte, um die bestehenden Probleme zu lösen. Klassisches klinisches Management umfasst bisher nicht IT-spezifische Patientenrisiken [vgl. 18, S. 132].

Es kann eine schwierige Vorstellung sein, (selbst oder mit einer Person) unter Lebensgefahr in ein Krankenhaus zu kommen, aber eine Behandlung ist kaum möglich, weil ein vermeidbarer IT-Angriff den Betrieb lahmlegt. Durch die in 2 beschriebene Methodik wurde keine Arbeit gefunden, welche die These in 1.4 beantwortet.

1.4 These

2017 gab es in Großbritanien durch WannaCry große Probleme in Krankenhäusern, obwohl der Angriff nicht auf sie gezielt war [vgl. 11, S. 1]. Wenn man die Nachrichten verfolgt, bekommt man auch in Deutschland von IT-Angriffen auf Kliniken mit. Berichterstattungen über die Vorfälle lenkten die Aufmerksamkeit des Autors auf die Thematik.

Das Essay untersucht folgende These: Es ist ein moralisch vertretbarer, verantwortungsvoller Prozess der Digitalisierung von Krankenhäusern in Deutschland durchführbar, wenn eine gesetzeskonforme IT-Sicherheit realisiert wird.

Es wird die Situation in Deutschland ausgewertet. Der zeitliche Rahmen ist begrenzt von 2015 bis zur Gegenwart. Diese Beschränkungen sollen eine genauere Betrachtung erlauben. Denn 2015 wurde das IT-Sicherheitsgesetz (für Deutschland) beschlossen und stellt damit ein wichtiges Jahr dar für die IT-Sicherheit im Land (siehe 3.5). Umsetzung angemessener IT-Sicherheit und Melden von Vorfällen wurde verpflichtet. Es wird die Lage betrachtet und bewertet, welche in Verbindung mit dem Gesetz existiert.

2 Methodik

Den in 3 aufgeführten Ergebnissen liegt eine theoretische, wissenschaftliche Arbeit zu Grunde. Zur Prüfung der in 1.4 beschriebenen These, wurde als qualitative Forschungsmethode die Literaturrecherche bzw. Literaturarbeit gewählt. Also die Sammlung und die Priorisierung von entsprechend für das Thema relevanter Literatur für eine folgende Erarbeitung des Themas. Dies entspricht der Befassung mit der aktuell vorhandenen wissenschaftlichen Literatur bzgl. Technikethik, sowie IT-Angriffen auf und Cyber Security in Krankenhäusern. Die Herangehensweise der Arbeit ist deduktiv, weil die bekannte Theorie auf einen Fall angewendet wird (durch logische Methoden).

Für die Literaturrecherche wurde eine Mischung aus dem systematischen und dem pragmatischen Vorgehen gewählt [vgl. 21, S. 50]. Bei der systematischen Weise wurde der Katalog der Hochschulbibliothek der THD („OPAC Deggendorf“) benutzt. Eine freie Suche im Katalog mit dem Stichwort „Technikethik“ führte zu dem Buch „Handbuch Technikethik“ [4].

Bei der pragmatischen Weise wurde „Google Scholar“ als Suchmaschine verwendet. Die Plattform half dabei Artikel aus (wissenschaftlichen) Fachzeitschriften zu finden, welche auf die aktuell bestehende IT-Sicherheit von Krankenhäusern, vergangene Cyber Attacken auf Krankenhäuser und auf die Chancen und Risiken der Digitalisierung in der Branche eingingen. Literatur, welche sich mit anderen security-spezifischen IT-Ausfällen beschäftigen, wurden auch in den Überblick mit einbezogen. Um die Literatur mit Hilfe von Google Scholar zu finden, wurden folgende Stichworte und entsprechende Synonyme, sowie verwandte

Wörter, verwendet: Krankenhaus, Technikethik, IT-Angriffe, IT-Sicherheit, Report. Weitere Literatur wurde durch die Schneeballmethode gesammelt, d.h. die so entstandene Literaturbasis ist durch selbst ausgewählte Titel aus den Literaturverzeichnissen der Funde weiter ergänzt worden [vgl. 21, S. 63]. Das Auffinden von „kma“-Artikeln, die mithilfe von Google Scholar ermittelt wurden, in der Wiso-Datenbank ermöglichte OPAC.

Die gefundenen, relevanten Quellen wurden dann im zweiten Schritt aufmerksam gelesen und inhaltlich ausgewertet, um einen Überblick über das Thema zu erlangen. Vor dem späteren Schreibprozess, wurden sie daraufhin auf die in 1.4 beschriebene These bezogen interpretiert.

Die Einschlusskriterien lauten: Es wurde nur Literatur zum Thema in Englisch oder Deutsch betrachtet und nur die deutsche Literatur, die auf die Situation in Deutschland eingeht, weil sich die These (1.4) auf Deutschland beschränkt. Für die zeitliche Beschränkung der These, musste Literatur über die Situation älter als 2014 sein.

Aktuellere Literatur wurde Älterer vorgezogen und wissenschaftliche Quellen wurden nicht-wissenschaftlichen Quellen bevorzugt. Außerdem wurden wissenschaftliche Fachzeitschriften bevorzugt angelesen, weil sie in der Wissenschaft eine hohe Bedeutung haben, aufgrund ihrer Aktualität [vgl. 21, S. 62]. Es wurde darauf geachtet Artikel aus unterschiedlichen wissenschaftlichen Quellen zu nehmen, um verschiedene Bewertungen zu erhalten und Einseitigkeit entgegenzuwirken sowie größtenteils wissenschaftliche Quellen zu verwenden, um gesicherte Informationen für die Ergebnisse zu erhalten.

3 Ergebnis

Noch bevor der Literaturrecherche aus 2 erfolgte eine pragmatische Suche [vgl. 21, S. 50] mit Google Scholar, Google und DuckDuckGo nach der IT-Sicherheits-Ausgabenhöhe oder IT-Fachkräfteanzahl von Kliniken über mehrere Jahre für eine (sekundäre) Datenauswertung. Geplant war diese als Indikator für die zeitliche Entwicklung der zugestandenen Relevanz von IT-Sicherheit zu betrachten. Das Ergebnis ist, dass die Suche für beide erfolglos war.

Die Literaturrecherche ergab überwiegend deutsche Quellen, weil sich die These auf Deutschland beschränkt (siehe 1.4) und die Einschlusskriterien (in 2) entsprechend formuliert wurden. Die Ergebnisse werden im Folgenden geordnet präsentiert. Die Ordnung hält sich an die Buchbeschreibung von „Handbuch Technikethik“ [4], welche im OPAC-Eintrag aufgeführt ist (Stand: 16.02.2022).

3.1 Vorteile der Digitalisierung

Die Krankenhaus-Digitalisierung hat großes Potenzial, z.B. können Behandlungen effizienter und einfacher werden [vgl. 6, S. V]. Viele Krankenhausabläufe werden

durch die Anwendung von vernetzten IT-Systemen besser [vgl. 10, S. 327]. Es besteht die Möglichkeit, Prozesse mehr aufeinander abzustimmen und miteinander zu vernetzen [vgl. 6, S. V]. Digitalisierung kann bestehende Strukturen effizienter gestalten, aber auch innovativ neuen Prozesse ermöglichen [vgl. 18, S. 132]. Die Patientenversorgung lässt sich qualitativ höherwertiger gestalten [vgl. 6, S. V]. Beispielsweise ist die kommende Elektronische Patientenakte für die medizinisch-pflegerische Arbeit sehr wertvoll [vgl. 14, S. 49]. Schutzziele wie die Patientensicherheit können stärker umgesetzt werden [vgl. 6, S. V]. Diese Verbesserungen sind erreichbar durch z.B. Automatisierung, umfangreichere Datenverarbeitung oder Expertise trotz räumlicher Trennung [vgl. 6, S. V]. Digitalisierung ermöglicht telemedizinischen Kontakt, Verfahrenssimulation mittels Virtual Reality, bessere Therapieentscheidungen, genauere Diagnostik, Roboterunterstützung etc. [vgl. 18, S. 132]. Im sozialen Bereich lässt sich die Kommunikation zwischen Patienten und Gesundheitspersonal erhöhen [vgl. 6, S. V].

Digitalisierung ist gut, weil der Nutzen durch sie moralisch zielführend ist. Sie hilft bei der Einhaltung der ethisch guten Schutzziele, verbessert Effizienz, Diagnosen und Behandlung.

3.2 Nachteile der Digitalisierung

IT-Sicherheitsmaßnahmen können negative Folgen für Abläufe haben, wie geringere Produktivität, Unzufriedenheit unter Beschäftigten oder Innovationshemmnisse [vgl. 22, S. 36]. Der Schaden von einem IT-Vorfall lässt sich nur schwer abschätzen, viel bleibt ungeklärt und nicht erfasst [vgl. 11, S. 1]. Durch IT-Sicherheitsvorgaben und Regeln kann man das Risiko eines IT-Vorfalls zwar verringern. Doch Sicherheitsmaßnahmen nerven viele Arbeitnehmer [vgl. 22, S. 36]. „Schulungen für mehr IT-Sicherheit sind bei Klinikmitarbeitern nicht beliebt“ [16, S. 66]. Manches Personal umgeht absichtlich IT-Sicherheitsvorgaben [vgl. 22, S. 36]. Es entstehen informelle Workarounds, d.h. Änderungen am vorgeschriebenen Ablauf ohne formale Genehmigung durchs Management [vgl. 18, S. 136]. Diese begünstigen erfolgreiche IT-Angriffe.

Es herrscht ein „akuter Fachkräftemangel in der Cybersecurity“ [19]. Trotz der in 3.6 aufgeführten Fortschritte in der Denkweise, kann die Umsetzung der nötigen Maßnahmen (z.B. Ausbesserung von Schwächen oder Schließen von Sicherheitslücken) zur Verminderung der Risiken langsam vorangehen. Die Anzahl an fehlenden Cybersecurity-Fachkräften (weltweit) wird im Millionen-Bereich geschätzt [vgl. 19].

Die Digitalisierung in deutschen Krankenhäusern gilt als rückständig [vgl. 6, S. V]. Sie kostet viel Geld und in die IT wird am wenigsten investiert [vgl. 13, S. 54]. 40 Prozent der deutschen Kliniken arbeiten (im klinischen Bereich) nicht digital [vgl. 20, S. 30]. Grund für den langsamen Wandel sind Datenschutzvorgaben und IT-Sicherheits-Richtlinien [vgl. 12, S. 102].

Digitalisierung bringt auch Nachteile mit sich, die nicht ignoriert werden dür-

fen. Denn Probleme in der IT-Sicherheit sind Probleme im Patientenschutz [vgl. 11, S. 1]. Neben hohen Kosten und wenig Fachkräften, ergeben sich auch (negative) Veränderungen für die Arbeit im Krankenhaus. Die Anforderungen steigen, weil mehr wichtige Vorgaben im Alltag zu beachten sind. Das Personal muss von ihren etablierten Arbeitsweisen wieder abweichen.

3.3 Chancen bzgl. IT-Sicherheit

2018 wurden neue Wege bei Schulungen gegangen, um dem Schulungsproblem aus 3.2 entgegenzuwirken, sodass die vermittelten, relevanten Informationen länger im Gedächtnis bleiben [vgl. 16, S. 66]. Innovative Ideen und effektivere Methoden als theoretische Seminare zur Informationsvermittlung sind möglich. Mithilfe von Planspielen können Verantwortliche lernen, wie man sich vor IT-Angriffe besser schützt [vgl. 16, S. 66].

Durch den Einsatz von modernen Techniken und Verfahren kann ein Krankenhaus ihre IT-Sicherheit erhöhen. Beispielsweise kann durch das Verwenden von einer sog. „Next-Generation Firewall“ Veränderungen im Netzwerkverkehr schnell erkannt werden [vgl. 8, S. 60].

Da Deutschland in der Digitalisierung Rückstand hat, kann man aus Erfahrungen und Wissen von anderen Ländern lernen und sehr erfolgreiche Technologien einkaufen [vgl. 1, S. 13]. Durch Gesetze kann man wirkungsvoll zu besserer Sicherheit verpflichten (siehe 3.6) [vgl. 22, S. 49].

3.4 Gefahren bzw. Risiken bei der IT-Sicherheit

IT-Kriminelle verursachen große Schäden [vgl. 22, S. 27]. Während z.B. ein OP-Fehler einen Patienten schaden kann, kann ein IT-Vorfall allen Patienten schaden [vgl. 11, S. 1]. Denn IT-Sicherheitsprobleme können mehr als eine Station betreffen, nämlich komplette Abteilungen, Kliniken oder Klinikverbünde [vgl. 18, S. 132]. Es entstehen häufiger neue Schwachstellen, wegen immer stärker vernetzten Medizingeräten und fehlendem IT-Schutz [vgl. 13, S. 54].

Krankenhäuser sind viel offener als (andere) Unternehmen und damit anfälliger für IT-Attacken. Hackern können, z.B. mittels eines offenen WLAN, in sie eindringen und bspw. Patientendaten manipulieren oder Medizingeräte kontrollieren [vgl. 20, S. 30]. Ein erfolgreicher Angriff basiert meistens auf Fehlern bei der Konfiguration oder der Benutzung (z.B. durch Angestellte) [vgl. 5, S. 50]. Fehlergründe bei der Benutzung sind oft fehlende oder inadäquate Schulungen (siehe 3.2) oder komplizierte Designs, Letzteres kann rasant zu Akzeptanzverlust führen [vgl. 18, S. 136]. Neben finanziellen Schäden sind auch Arbeitsausfälle oder Reputationsschäden die Folgen von Sicherheitsvorfällen [vgl. 22, S. 27]. Das Einsetzen von digitalen Patientenakten erhöht nicht nur den Patientenschutz, sondern kann ihn auch verringern, weil ein IT-Angriff mehr betriebsnotwendige Informationen betrifft [vgl. 13, S. 53].

Diese Gefahren und Risiken sind schwerwiegend. Ein Risikomanagement ist essentiell, um einen Zustand zu erreichen, welcher eine moralisch vertretbare Auskostung der Vorteile aus 3.1 erlaubt. Zur Verminderung der Risiken gibt es viele Möglichkeiten (3.3) und das etablierte Forschungsfeld Cyber Security. Diese können als ein Mittel zum Zweck angesehen werden die Verantwortung wahrzunehmen und den Zustand zu erreichen.

3.5 Sicherheit

Es gilt, dass keine 100% IT-Sicherheit erreichbar ist [vgl. 8, S. 60]. Aber es muss eine angemessene Sicherheit hergestellt werden. 2015 trat in Deutschland das IT-Sicherheitsgesetz in Kraft, zur Erhöhung der IT-Sicherheit in „Kritischen Infrastrukturen“, zu denen Krankenhäuser zählen [vgl. 22, S. 48]. Damit sind sie verpflichtet weitergehende Regeln zur IT-Sicherheit und zum Umgang mit Vorfällen einzuhalten [vgl. 9, S. 7].

Mit Betrachtung der Vorteile (3.1) und Gefahren (3.4) gilt: Digitalisierung kann die Patientensicherheit stark verbessern, aber durch IT-Schwächen oder falsche Verwendung können große Sicherheitsrisiken entstehen [vgl. 18, S. 129]. Um die Patientensicherheit schlussendlich zu erhöhen, braucht es kontinuierliche Zusammenarbeit zwischen Produzenten, Betreibern und Endanwendern [vgl. 18, S. 129]. Auch Bürgervertrauen ist ein wichtiger Faktor. Ein Grundvertrauen in Entscheidungsträger und Lösungen ist essenziell für die Implementierung von Maßnahmen, wie der Elektronischen Patientenakte, aber dieses fehlt bei Vielen [vgl. 1, S. 13].

3.6 Fortschritt

Viele Verantwortliche finden gesetzliche Regulierungen und Verpflichtungen (z.B. das IT-Sicherheitsgesetz aus 3.5) wirksam, wichtig und unterstützend bei der Umzusetzung und Vertretung von IT-Sicherheitsmaßnahmen [vgl. 22, S. 49]. Mittels „Krankenhauszukunftsgesetz“ werden mehrere Millarden Euro zur Investition in IT-Sicherheit, Notfallkapazitäten und Digitalisierung bereitgestellt [vgl. 2, S. 316]. Bayern initierte Straferhöhungen für IT-Angriffe auf Krankenhäuser [vgl. 2, S. 330]. Der erste Schritt, das Erkennen, dass es ein Problem gibt, findet statt. Manager haben die Wichtigkeit von effektiver Cyber Security erkannt [vgl. 22, S. 52]. Doch neben wichtigen Investitionen in IT-Sicherheit, ist gerade eine Änderung der Organisationskultur (z.B. Personalverhalten) essentiell [vgl. 11, S. 1]. Auch in Messverfahren gab es Entwicklungen. Neue Methodiken wurden entwickelt, zur besseren Analyse der IT-Sicherheit (z.B. das HITS Framework) [vgl. 18, S. 133].

Es gibt Fortschritte in vielen Bereichen (technisch, personell, regulatorisch etc.). Verantwortliche (3.7) sorgen durch Handelungen für eine Verbesserung der

Situation. Ob diese effektiv sind und wie sich die Situation weiter entwickelt, wird die Zukunft zeigen.

3.7 Verantwortung

Verantwortliche sind die in 3.5 genannten Produzenten, Betreiber, Endanwender und der Staat. Die Betreiber rechnen der IT-Sicherheit eine hohe Relevanz zu [vgl. 22, S. 16]. Im Gesundheitswesen ist das IT-Sicherheitsgesetz noch mit am bekanntesten [vgl. 22, S. 48]. Der Staat muss die gesundheitliche Versorgung der Bürger gewährleisten [vgl. 7, B63]. Bei der Verwendung von Computern müssen effektive IT-Sicherheitsmanagement-Prozesse existieren [vgl. 20, S. 30].

Das Bewusstsein über die Gefahren nimmt zu [vgl. 22, S. 18]. Verantwortliche nehmen ihre Verantwortung war und handeln (siehe 3.6), z.B. werden Gesetze entwickelt.

4 Fazit

Die Krankenhaus-Digitalisierung bringt viele große Vorteile mit sich. Aber auch Nachteile, wie hohe Kosten und erstzunehmende Gefahren. Die Patientensicherheit ist von der IT-Sicherheit abhängig. Es sind die elementaren Schutzziele der Informationssicherheit bedroht. Dazu zählt Vertraulichkeit der Daten (und damit auch Datenschutz), Integrität der Daten, z.B. durch (böswillige) unberechtigte Manipulation und Verfügbarkeit der Daten, z.B. durch IT-Ausfälle oder Verschlüsselung. Damit ist auch das klinische Schutzziel Patientensicherheit bedroht. Erschwerend kommt hinzu, dass der IT-Sicherheits-Fachkräftemangel nicht nur Krankenhäuser betrifft, sondern auch viele Unternehmen in Deutschland, durch ihn ist die IT-Sicherheit bei Vielen schlechter als gesetzlich vorgeschrieben [vgl. 22, S. 28]. Dabei konkurrieren Krankenhäuser mit Firmen auf dem Arbeitsmarkt um Fachkräfte.

Da die Anwendung eines der größten Probleme darstellt, ist hier eine Verbesserung des Verhaltens bzw. der Umstände unbedingt nötig. Dabei müssen aber auch die Hersteller und Betreiber in Verantwortung gezogen werden, für z.B. gutes, intuitives Programm-Design und Kommunikation. Eine Absprache mit den Anwendern, das Personal, ist wichtig. Man sollte ihnen eine Entscheidung und Meinung zugestehen, bei der Gestaltung ihres Arbeitsplatzes und ihrer Arbeitsabläufe. Dabei kann man vorher abklären was sie mitmachen würden und was nicht. Sodass man Entscheidungen über sie auch mit ihnen trifft. Außerdem ist Aufklärung wichtig z.B. über den Sinn von Maßnahmen oder die IT-Angriffsmethoden.

Es gibt wesentlichen Fortschritt durch Verantwortliche, sie haben die Wichtigkeit von IT-Sicherheit erkannt und probieren ihr gerecht zu werden. Unterstützt werden sie durch das global bedeutende Forschungsfeld IT-Sicherheit.

Generell ist die (Krankenhaus-)Digitaliserung kaum aufhaltbar. Wenn man eine effektive IT-Sicherheit umsetzt, so wie es gesetzlich vorgeschrieben ist, dann minimiert man entstehende Risiken der Digitaliserung. Durch diese Minimierung wird man seiner Verantwortung (Leben und Privatsphäre zu schützen) nach gesellschaftlichen Maßstab gerecht. Mit behandelten Risiken ist der Prozess damit moralisch vertretbar, weil man auch verantwortungsvoll agiert. Die These (1.4) ist somit zutreffend.

5 Referenzen

Literatur

[1] Nick Bertram u. a. „Einführung einer elektronischen Patientenakte in Deutschland vor dem Hintergrund der internationalen Erfahrungen“. In: *Krankenhaus-Report 2019: Das digitale Krankenhaus*. Hrsg. von Jürgen Klauber u. a. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2019, S. 3–16. ISBN: 978-3-662-58225-1. DOI: 10.1007/978-3-662-58225-1_1.

[2] Dirk Bürger und Martina Purwins. „Krankenhauspolitische Chronik“. In: *Krankenhaus-Report 2021: Versorgungsketten – Der Patient im Mittelpunkt*. Hrsg. von Jürgen Klauber u. a. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2021, S. 309–348. ISBN: 978-3-662-62708-2. DOI: 10.1007/978-3-662-62708-2_17.

[3] Guntram Doelfs. „Cybersecurity: Sicherheitsrisiko Krankenhaus“. In: *kma-Klinik Management aktuell* 26.04 (2021), S. 22–27. DOI: 10.1055/s-0041-1729370.

[4] Armin Grunwald und Rafaela Hillerbrand. *Handbuch Technikethik*. 2. Aufl. J.B. Metzler, 2021. ISBN: 9783476049001.

[5] Thomas Jäschke. „Krankenhaus gehackt—wie sicher ist unsere IT?“ In: *Heilberufe* 69.1 (2017), S. 49–51. DOI: 10.1007/s00058-017-2578-0.

[6] Jürgen Klauber u. a. *Krankenhaus-Report 2019: Das digitale Krankenhaus*. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2019. ISBN: 9783662582251. DOI: 10.1007/978-3-662-58225-1.

[7] Peter Knuth. „Besser spät als gar nicht“. In: *Notfall & Hausarztmedizin (Hausarztmedizin)* 31.03 (2005), B–63. DOI: 10.1055/s-2005-869499.

[8] Martin Kucera. „IT-Sicherheit:„Absolute Sicherheit gibt es nicht““. In: *kma-Klinik Management aktuell* 24.10 (2019), S. 60–61. DOI: 10.1055/s-0039-1700425.

[9] Sascha Maier und Sandra Aengenheyster. „Cyber-Security und Resilienz verstehen“. In: *Geschäftsrisiko Cyber-Security: Leitfaden zur Etablierung eines resilienten Sicherheits-Ökosystems*. Wiesbaden: Springer Fachmedien Wiesbaden, 2020, S. 1–13. ISBN: 978-3-658-32046-1. DOI: 10.1007/978-3-658-32046-1_1.

[10] Matthias Manych. „Digital vulnerabel–Krankenhäuser zwischen IT-Chancen und -Angriffen“. In: *Zeitschrift für Orthopädie und Unfallchirurgie* 158.04 (2020), S. 327–328. DOI: 10.1055/s-0037-1599646.

[11] Guy Martin u. a. „WannaCry—a year on“. In: *The BMJ* 361 (2018). DOI: 10.1136/bmj.k2381.

[12] David Matusiewicz, Jana Aulenkamp und Jochen A. Werner. „Effekte der digitalen Transformation des Krankenhauses auf den Wandel des Berufsbildes Arzt“. In: *Krankenhaus-Report 2019: Das digitale Krankenhaus*. Hrsg. von Jürgen Klauber u. a. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2019, S. 101–114. ISBN: 9783662582251. DOI: 10.1007/978-3-662-58225-1_8.

[13] Dirk Mewis. „IT-Sicherheitslücken: Cybercrime in deutschen Krankenhäusern“. In: *kma-Klinik Management aktuell* 22.10 (2017), S. 53–56. DOI: 10.1055/s-0036-1594863.

[14] Julia Oswald und Klaus Goedereis. „Voraussetzungen und Potenziale des digitalen Krankenhauses“. In: *Krankenhaus-Report 2019: Das digitale Krankenhaus*. Hrsg. von Jürgen Klauber u. a. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2019, S. 49–66. ISBN: 978-3-662-58225-1. DOI: 10.1007/978-3-662-58225-1_4.

[15] Norbert Pohlmann. „IT-Sicherheit IM Krankenhaus: Ohne Cybersicherheit gelingt keine nachhaltige Digitalisierung“. In: *kma-Klinik Management aktuell* 24.10 (2019), S. 55–59. DOI: 10.1055/s-0039-1700424.

[16] Andreas Rieb. „IT-Sicherheit: Cyberabwehr mit hohem Spaßfaktor“. In: *kma-Klinik Management aktuell* 23.07/08 (2018), S. 66–69. DOI: 10.1055/s-0036-1595355.

[17] Stefan A. Seeger. *Verantwortung: Tradition und Dekonstruktion*. Bd. 482. Königshausen & Neumann, 2010. ISBN: 9783826042713.

[18] Eva Sellge und Ernst-Günther Hagenmeyer. „Digitalisierung und Patientensicherheit“. In: *Krankenhaus-Report 2019: Das digitale Krankenhaus*. Hrsg. von Jürgen Klauber u. a. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2019, S. 129–144. ISBN: 9783662582251. DOI: 10.1007/978-3-662-58225-1_10.

[19] Anne Steinbach. „Cybersecurity ist endlich Chefsache“. In: *Controlling & Management Review* 63.8 (2019), S. 69. DOI: 10.1007/s12176-019-0074-x.

[20] Victor Stephani, Reinhard Busse und Alexander Geissler. „Benchmarking der Krankenhaus-IT: Deutschland im internationalen Vergleich“. In: *Krankenhaus-Report 2019: Das digitale Krankenhaus*. Hrsg. von Jürgen Klauber u. a. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2019, S. 17–32. ISBN: 9783662582251. DOI: 10.1007/978-3-662-58225-1_2.

[21] Manuel René Theisen und Martin Theisen. *Wissenschaftliches Arbeiten: Erfolgreich bei Bachelor- und Masterarbeit*. 18. Aufl. Vahlen, 2021. ISBN: 9783800663736.

[22] TÜV. *TÜV Cybersecurity Studie*. Forschungsber. TÜV-Verband, 2019.

[23] Thomas Wurmb u. a. „Vollausfall der Informationstechnologie im Krankenhaus“. In: *Der Unfallchirurg* 123.6 (2020), S. 443–452. DOI: 10.1007/s00113-020-00797-4.