Digitalisierung im Gesundheitswesen:
Steigerung des Patientenwohls durch vertrauenswürdige und sichere Verarbeitung von medizinischen Daten

PROF. NORBERT POHLMANN; INSTITUT FÜR INTERNET-SICHERHEIT (POHLMANN@INTERNET-SICHERHEIT.DE)

DR.-ING. TOBIAS URBAN; INSTITUT FÜR INTERNET-SICHERHEIT, SECUNET SECURITY NETWORKS AG (URBAN@INTERNET-SICHERHEIT.DE)

Das Gesundheitswesen in Deutschland, Europa, aber auch weltweit steht gerade erst am Beginn eines notwendigen und besonderen Digitalisierungsschubs. Ein wichtiger Schritt im Rahmen dieser Digitalisierung wird es sein, sämtliche medizinische Daten leistungsträgerübergreifend einfach verfügbar zu machen. Dies ermöglicht neue Methoden der Behandlung wie durch KI-Ansätze oder die Vermeidung von Doppelbehandlungen. Zur Erreichung dieser Ziele ist es unabdingbar, dass moderne medizintechnische IT-Geräte miteinander vernetzt werden und die anfallenden Daten sicher verarbeitet und hinterlegt werden. Durch diesen Prozess entstehen aber auch neue Angriffsvektoren und die Risiken steigen erheblich an.

Diese Arbeit beschreibt zunächst grundlegende Cyber-Sicherheitsstrategien, die helfen die vorhandenen Risiken zu minimieren und mit den verbleibenden Risiken umzugehen. Zusätzlich werden konkrete Sicherheitsbedürfnisse- und Anforderungen, die zur Vernetzung von Medizintechnik und zur Verarbeitung von Daten in der Cloud, nötig sind diskutiert. Abschließend wird eine Gesamtarchitektur vorgestellt, die diese Sicherheitsbedürfnisse umsetzt.

1. Einführung

Informationstechnik und das Internet sind Motor und Basis für das Wohlergehen der modernen und globalen Informations- und Wissensgesellschaft. Das gilt auch für das Gesundheitswesen insgesamt und für Krankenhäuser insbesondere. Die moderne Medizin wird viel stärker als bisher auf Daten angewiesen sein, die aus vielfältigen Quellen zu einem Patienten gesammelt werden. Diese sind beispielsweise Medizintechnik, ärztliche Befundungen, Diagnosen und Daten aus medizinischen Fitness Apps. Diese Daten müssen leistungsträgerübergreifend verfügbar und jederzeit zugänglich gemacht werden, um das volle Potential digitaler Gesundheitsanwendungen und insbesondere von *Künstlicher Intelligenz* (KI) nutzbar zu machen. Ziel der Digitalisierung des Gesundheitswesens ist also die Schaffung von Diensten, die nachhaltig die Versorgung der Partien verbessern und vereinfachen, um den Menschen als zentralen Punkt im Gesundheitswesen zu setzen.

Dieser globale Trend ist auch in Deutschland zu beobachten und wird aktiv vorangetrieben. Beispiele hierfür sind: Die elektronische Patientenakte, die Daten für alle und überall verfügbar machen soll; die Forderung nach virtuellen Krankenhäusern aus der Politik; der vermehrten Nutzung von Telemedizin oder Konsultation des Arztes in virtuellen Sprechstunden.

Die so zu erwartende deutliche Steigerung der Versorgungsqualität bedingt allerdings aus Sicht der IT-Sicherheit verschiedene Herausforderungen. Eine von der *U.S. Food and Drug Administration* (FDA) in Auftrag gegeben Studie zeigt auf, dass jedes medizintechnische Gerät im Mittel 6,2 Schwachstellen aufweist und Medizintechnik immer stärker in das Visier von Angreifenden gerät (Frost & Sullivan, 2019). Ebenfalls in den USA musste ein Krankenhaus für den Datenverlust von medizinischen Daten 5,5 Mio. US-Dollar Strafe zahlen (Heise online, 2016). Zwar sind die in Deutschland verhängten Strafen bzw. aufgetretenen finanzielle Schäden für solche Vorfälle nicht ansatzweise so hoch, trotzdem geht der Schaden durch erfolgreiche Ransomware Angriffe auf Krankenhäuser in die Millionen.

2. Herausforderungen der Digitalisierung im Gesundheitswesen

Zur Umsetzung einer modernen personalisierten Medizin ist die vertrauenswürdige Erfassung von medizinischen Daten leistungserbringerübergreifend bis hin in das heimische Umfeld von Patienten nötig („Hospital-to-Home“). Daten aus unterschiedlichen Quellen müssen einheitlich erfasst und nutzbar gemacht werden. Aus Sicht der IT-Sicherheit ergeben sich so vielfältige Herausforderungen.

Auf der einen Seite stehen Anforderungen an den Datenschutz, beispielsweise gefordert durch die

Datenschutz-Grundverordnung (DSGVO) oder das *Patientendaten-Schutz-Gesetz* (PDSG). Auf der anderen Seite wird die Selbstbestimmung der Patienten zum Umgang mit den eigenen Daten weiter in den Vordergrund rücken, um sicherzustellen, dass die erhobenen Daten nur für die benötigten Zwecke wie die Behandlung genutzt werden bzw. eine Weiternutzung beispielsweise für die Forschung nur mit explizitem Einverständnis möglich ist. In diesem Sinne ist die Transparenz und Nachverfolgbarkeit, das heißt wer hat wann welche Daten zu welchem Zweck genutzt, unabdingbar, um Vertrauen in ein solches Gesundheitssystem aufzubauen.

Andererseits wird durch die Vernetzung aller Teilnehmer die Angriffsfläche deutlich größer und es entstehen neue Angriffsvektoren. Konkret bedeutet dies beispielsweise für Krankenhäuser, dass Medizintechnik, die, um Daten zur Verfügung zu stellen, an das Internet angeschlossen wird, Ziel von modernen Angriffsvektoren werden kann. Dazu kommt, dass die Nutzungszeit von medizinischen Großgeräten oft weit über den gängigen Empfehlungen, wie lange IT-Sicherheitstechnologie sicher genutzt werden können, liegt.

Der Trend hin zu immer mehr Cloud Lösungen („off-premises“) stellt Leistungserbringer vor weitere Probleme. Gängige Lösungen der sog. Hyperscaler wie *Azure*, *AWS* und *Google* werden weder den rechtlichen Anforderungen noch den Forderungen nach Vertrauenswürdigkeit und Sicherheit in Bezug auf Gesundheitsdaten gerecht.

Auf nicht technischer Seite werden die Behandelnden, Pflegenden und weiteres Personal bei den Leistungserbringern weiter in den Fokus der Angreifer rücken, zum Beispiel um Daten zu exaltieren. Lösungsansätze können also nicht nur technischer Natur sein, sondern müssen vielmehr holistisch sein.

2.1. Mit passenden Cyber-Sicherheitsmechanismen den Betrieb eines Krankenhauses schützen

Das heißt, die Krankenhäuser brauchen passende Cyber-Sicherheitsmechanismen, um sich angemessen zu schützen und damit ihren eigentlichen Auftrag sicher und vertrauenswürdig umsetzen zu können.

Ein technisch ganzheitliches Sicherheitskonzept muss die „Orte”, an dem die Daten erhoben werden wie an der Medizintechnik beginnen und alle Punkte, an den diese weiterverarbeitet werden wie „edge-Computing” bis hin in die digitalen Gesundheitsanwendungen in der Cloud abdecken. Dabei muss IT-Sicherheit auf allen Ebenen gedacht werden und über einzelne IT-Sicherheitsmaßnahmen wie eine verschlüsselte Verbindung weit hinausgehen. Zur Sicherstellung der Integrität der ausgeführten Anwendungen und der Vertraulichkeit der übertragenen und zu verarbeitenden Daten muss ab der Hardware, über einen Vertrauensanker („Root of Trust”), beginnend eine Vertrauensbeziehung hergestellt werden. Hinzukommen organisatorische Maßnahmen wie Richtlinien, Vorfallsreaktionen, Meldewege und weitere Anforderungen, die aufgrund diverser Regularien notwendig sind, aber auch personelle Maßnahmen wie Schulung der Mitarbeitenden, die Sicherheitsbewusstsein schaffen und den Umgang mit Informationen sensibilisieren.

3. Lösungsansätze

Im Folgenden werden Lösungen zur Behebung der beschriebenen Herausforderungen diskutiert. Dabei werden zunächst allgemeine Cyber-Sicherheitsstrategien ausgeführt. Anschließend wird eine konkrete Architektur inklusive der Komponenten vorgestellt, die eine moderne aber immer noch sichere und vertrauenswürdige Erfassung und Verarbeitung medizinischer Daten ermöglicht.

3.1. Cyber-Sicherheitsstrategien

Wie beschrieben vergrößert sich durch die Digitalisierung im Gesundheitswesen die Angriffsfläche und somit steigt auch das Risiko eines Schadens, weil die Angriffsziele immer lukrativer werden. Für eine strategisch nachhaltige Reduktion dieser Situation müssen grundsätzliche Sicherheitsstrategien umgesetzt werden, die zum einen das bestehende Risiko reduzieren und zum anderen mit verbleibenden Restrisiken umzugehen (siehe auch beispielhaft Abbildung 1). Im Folgenden werden vier grundsätzliche Strategien beschrieben, die helfen diese Ziele zu erreichen.

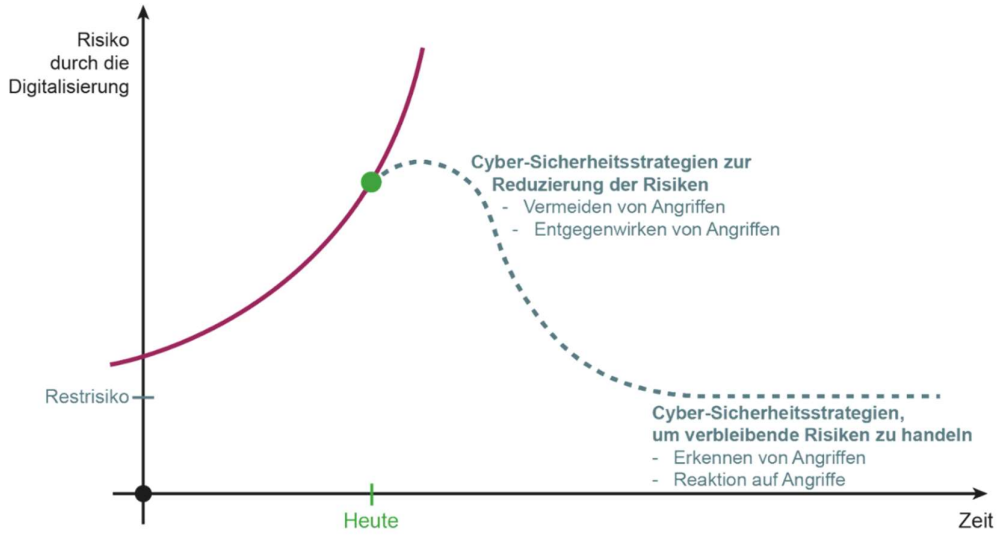

Abb. 1 : Cyber-Sicherheitsstrategien, um die Risiken der Digitalisierung zu managen

3.1.1. Vermeiden von Angriffen

Ein allgemeiner Ansatz zum Schutz von sensiblen Daten ist, die Angriffsfläche zu minimieren und damit eine Reduktion des Risikos zu erreichen (Pohlmann, 2019). Im Gesundheitswesen sind hier insbesondere das Prinzip der Datensparsamkeit - so wenige wertvolle Daten generieren wie möglich und so viele wie nötig, die Fokussierung von schützenswerten Daten auf sehr wenige IT-Systeme, die Reduzierung von IT-Möglichkeiten wie nicht notwenige Software sowie nicht verwendete Funktionen in einer Anwendung und sicherheitsbewusste Mitarbeitende erfolgsversprechende Ansätze erfolgreich Angriffe zu vermeiden. Ein Beispiel für diese Strategie ist es, die genutzten Systeme im Krankenhaus zu überprüfen und Systeme, die nicht länger gebraucht werden, abzuschalten. Nicht mehr im Gebrauch befindliche Systeme werden oft nicht mehr administriert und sind damit häufig Einfallstore für die Angreifenden.

3.1.2. Entgegenwirken von Angriffen

Die am meisten verwendete Strategie zur Reduktion des Schadens durch Angriffe ist das *Entgegenwirken* gegen mögliche Angriffsvektoren. Hierzu zählen gängige Verfahren wie der Einsatz von starker Verschlüsselung, Anti-Malware Lösungen, digitale Signatur, Anti-DDoS-Verfahren oder sichere Authentifikationsverfahren wie Multifaktor Verfahren. Zur Umsetzung dieser Strategie kann zum Beispiel eine Lösung zum Einsatz kommen, die den Datenverkehr von (alter) Medizintechnik direkt am Gerät verschlüsselt und somit die Übertragung der sensiblen Daten über das Netzwerk schützt.

3.1.3. Erkennen von Angriffen und Reaktion auf Angriffe

Keine IT-Sicherheitsmaßnahme kann vollständigen Schutz garantieren. Daher ist das *Erkennen von Angriffen und die Reaktion* darauf ein wichtiger Bestandteil eines jeden Sicherheitskonzepts. In dem Bereich der Erkennung von Angriffen spielen Frühwarnsysteme wie *Intrusion Detection Systeme* (IDS) eine zentrale Rolle. Wenn Angriffe erkannt werden, sollte so schnell wie möglich mit passenden Aktionen reagiert werden, die den Schaden im optimalen Fall noch verhindern oder zumindest die Höhe reduzieren. Wichtig ist auch, dass es bereits ein getestetes Reaktionskonzept (Notfallplanungen) gibt, in dem definiert ist, was im Krisenfall die richtige Vorgehensweise ist und welche Personen die Rechte haben, die entsprechenden Reaktionen im Angriffsfall auszulösen. Besonders relevant ist dabei, alle definierten Reaktionen sehr gut gemeinsam zu trainieren, damit in einem Ernstfall die adäquaten Reaktionen schnell und erfolgreich umgesetzt werden können.

3.2. Konkrete Lösungsansätze

Langfristig wird ein neues Gesundheitsökosystem benötigt, dass alle IT-Systeme im Gesundheitswesen eigenständig einschließt und direkt die notwendigen IT-Sicherheitsmechanismen auf dem Stand der Technik integriert, um flexibel auf die veränderten Herausforderungen reagieren zu können. Auf diesem Weg müssen aber noch Zwischenschritte und Konzepte umgesetzt werden, damit die heutigen besonders wichtigen Herausforderungen sicher und vertrauenswürdig umgesetzt werden können.

Neben den gerade beschrieben allgemeine Strategien zur Reduktion der Angriffsfläche und zur Reaktion auf erkannte Angriffsvektoren wird im Folgenden eine Architektur dargestellt, die es erlaubt – aus Sicht der IT-Sicherheit – medizinische Daten, die im Krankenhaus oder bei anderen Leistungserbringern anfallen sicher und vertrauenswürdig in Cloud-Umgebungen zu verarbeiten. Die Architektur unterscheidet dabei zwischen der Datenverarbeitung auf eigenen Servern in den Räumlichkeiten des Krankenhauses („on-premises“) und der Datenverarbeitung in der Cloud, bei der sämtliche Daten auf externen Servern eines Cloud-Anbieters gespeichert sind („off-premises“).

3.2.1. Datenerfassung- und Verarbeitung im Krankenhaus

Eine der Größten Herausforderungen bei der Vernetzung und Digitalisierung von Medizintechnik zum *Internet of Medical Things* (IoMT) sind die langen Einsatzzeiten dieser. IT-Sicherheitslösungen müssen also zum einen in der Lage sein, veraltete Geräte sicher in ein Netzwerk zu integrieren und zum anderen sicherzustellen, dass diese immer durch den aktuellen Stand der Technik geschützt werden. So sind beispielsweise 60% der medizintechnischen Geräte im Feld „End of Life“, und werden entsprechend nicht mehr gewartet also u.a. auch nicht mehr mit Sicherheitsupdates versorgt (Frost & Sullivan, 2019).

Für eine nachhaltig sichere Vernetzung muss entsprechend direkt am/im Gerät bzw. für eine kleinen Gruppe von Geräten Sicherheitstechnologie entstehen, die diese und den medizinischen Prozess schützt und im Bedarfsfall isolieren kann. So wird die IT-Sicherheitsfunktionalität lose an das IoMT Geräte gekoppelt, was einen sicheren und vertrauenswürdigen Betrieb ermöglicht, auch wenn das Gerät nicht mehr als sicher eingestuft werden kann. Dies würde auch den Vorteil bringen, dass nicht direkt in die medizinische Funktionalität des Geräts eingegriffen wird. Ebenfalls müssen, wie bereits heute schon häufig in Ansätzen zu erkennen ist, klare Zonenkonzepte für IIoMT Geräte und andere Krankenhaus IT erstellt werden, die helfen, die Angriffsfläche zu verkleinern. Dabei würde der Schaden auf einzelne Zonen wie beispielsweise gewöhnliche IT in der Radiologie oder IIoMT im OP-Saal reduziert werden.

Durch spezielle IT-Sicherheitsgateway Technologien können diese Zonen zentral („on-the-edge”) zusammengeführt und die Daten Mehrwertdiensten zugänglich gemacht werden, ohne die Krankenhaus IT zu stark zu öffnen. Dieses zentrale Gateway, das hochsensible Daten aus verschiedenen und Quellen und IoMT Geräten konsolidiert ist somit eine besonders kritische und schützenswerte Komponente. Diese Komponente dient aber auch als mögliche Schleuse zu Ausweitung von anonymisierten bzw. pseudonymisierten Daten in die Cloud, in der die Daten von digitalen Gesundheitsanwendungen nutzbar gemacht werden können. Die Komponente eignet sich auch um Anwendungen, wie ein „on-the-edge“ zu betrieben und zu schützen.

3.2.2. Datenverarbeitung in der Cloud

Neben rechtlichen Hürden wie der DSGVO, der ärztlichen Schweigepflicht oder der PDSG sind auch auf der technischen Seite unterschiedliche Herausforderungen zu meistern, wenn Gesundheitsdaten in der Cloud verarbeitet werden sollen. Aufgrund der hohen Sensibilität der zu verarbeitenden Daten muss für die Cloudumgebungen, auf der digitale Gesundheitsanwendungen betrieben werden, ein Höchstmaß an IT-Sicherheit umgesetzt werden – die deutlich über das gängiger Cloud Anbieter hinausgeht. Das Ziel muss sein, dass über Ansätze wie *Confidential Computing* und *Trusted Exekution Environments* (Sabt, 2015) ein vertrauenswürdiger logischer Kanal von dem Patienten bis hin zu den Applikationen in der Cloud und den Prozessoren, die letztlich die Daten verarbeiten entsteht und dieser nicht unbemerkt kompromittiert werden kann. *Trusted Exekution Environments* sollen dabei sicherstellen, dass eine starke Separierung und

Isolierung unterschiedlicher Softwarekomponenten, wie beispielsweise Krankenhausinformationssysteme unterschiedlicher Leistungserbringer, einfach auf einem zentralen Cloud System umgesetzt werden können. Da die Applikationen in der Cloud mit hochsensiblen Daten arbeiten sollten diese selbstverständlich jederzeit verschlüsselt sein. Dabei ist zu beachten, dass jegliche Schlüssel nur im Besitz der Leistungserbringer sind und nicht von den Cloud-Anbietern eingesehen werden können. Dies wird unter dem Begriff „Bring and hold your own key“ zusammengefasst.

3.2.3. Darstellung einer IT-Sicherheitsarchitektur für Gesundheitsplattformen

Die im Vorherigen beschriebenen Ansätze werden in diesem Abschnitt zu einer Gesamtarchitektur kombiniert, die es erlaubt eine Plattformökonomie im Gesundheitswesen sicher und vertrauenswürdig umzusetzen. Eine solche Ökonomie muss mindestens die folgenden Aufgaben erfüllen:

(1) sichere Erfassung und Übertragung von medizinischen Daten,

(2) vertrauensvolle Verarbeitung von medizinischen Daten,

(3) Umsetzung eines geeigneten Konzepts zur digitalen Selbstbestimmung und

(4) ein Rechte- und Zugriffskonzept auf die erhobenen Daten im Einklang mit Punkt Drei.

Da Punkt drei und vier nicht direkt von der Architektur umgesetzt werden – diese aber ermöglichen müssen – werden diese Punkte im Folgenden nicht weiter beschrieben. Abbildung 2 zeigt die Architektur beispielhaft auf.

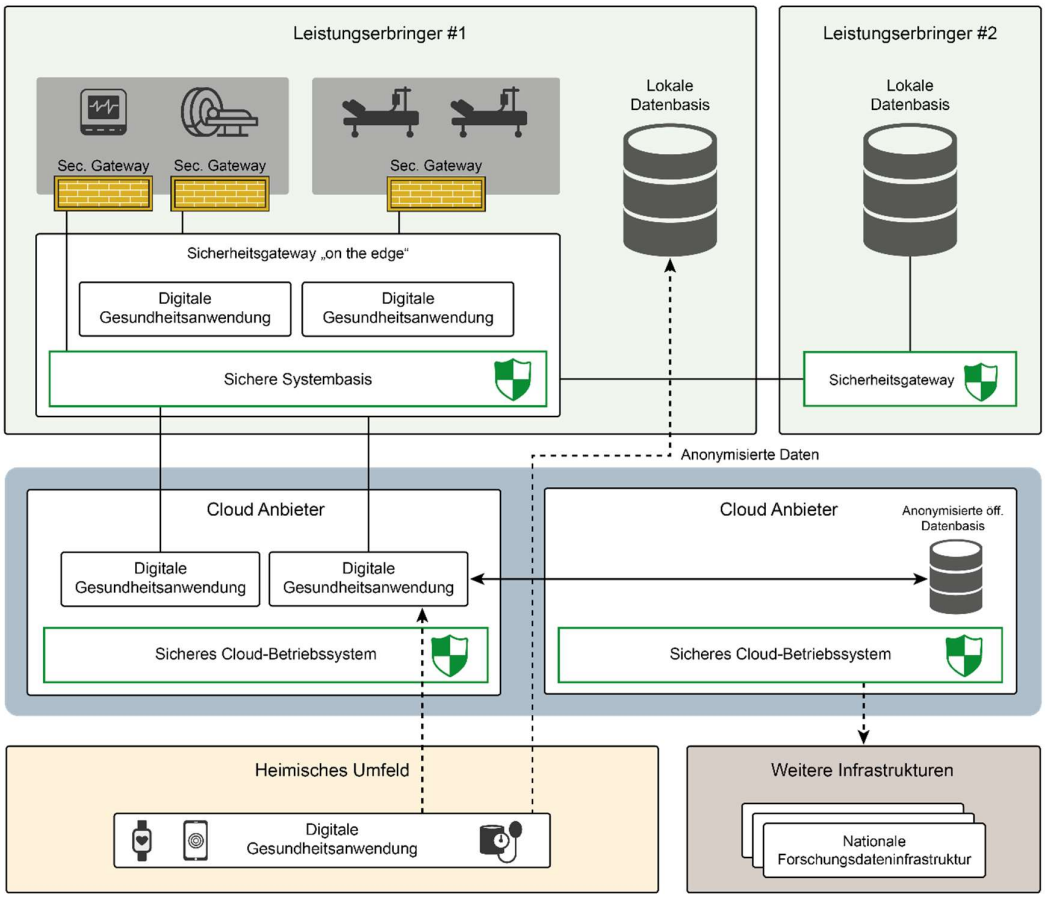

Abb. 2 Schematische Darstellung einer Architektur die eine sichere und vertrauenswürdige Umsetzung einer Gesundheitsplattform erlaubt.

Sichere Erfassung und Übertragung von Medizinischen Daten

Grundlegend werden behandlungsrelevante Daten in Zukunft nicht nur bei den Leistungserbringern anfallen, sondern vermehrt auch im heimischen Umfeld der Patienten zum Beispiel über medizinische Fitness Tracker, die sicher und vertrauenswürdig mit den Behandelnden bei den Leistungserbringern geteilt werden müssen. Das Sicherheitsgateway am Rande des Netzwerkes ermöglicht die Umsetzung des vertrauenswürdigen Einschleusens der sensiblen Daten und der Überführung dieser in die lokale Datenbasis. Ebenfalls könnte so eine direkte Live-Übermittlung von Daten aus dem heimischen Umfeld der Patienten umgesetzt werden und eine echte bedarfsgerechte und personalisierte Medizin sicher umgesetzt werden. Neben der Erfassung der Daten aus dem heimischen Umfeld können über die zentrale Komponente auch die Daten, die direkt bei dem Leistungserbringer anfallen oder die bei anderen Leistungserbringern angefallen sind, konsolidiert werden. Dafür können in Zukunft Mechanismen der Telematikinfrastruktur 2.0 (gematik, 2020) genutzt werden. Die Medizintechnik kommuniziert über die dezidierte Sicherheitskomponente direkt am Gerät mit dem zentralen Gateway oder mit Cloud-Diensten (z.B. zur Fernwartung oder zur Einspielung von Updates). Ebenfalls werden die Geräte so innerhalb der eigenen Sicherheitszone, die von dem zentralen Gateway aufgebaut wird, zusätzlich geschützt bzw. können im Bedarfsfall einfach isoliert werden. Ebenfalls ist denkbar das auf diesen Komponenten direkt Anwendungen mit medizinischem Mehrwert wie Überwachung von Vitaldaten vertrauensvoll ausgeführt werden.

Vertrauensvolle Verarbeitung von Medizinischen Daten

Die Verarbeitung von medizinischen Daten in Cloudumgebungen wird auch aufgrund der zu erwartenden benötigen Ressourcen unabdingbar sein. Es ist nicht sinnhaft, dass jeder Leistungserbringer eine eigene Hochleistungsinfrastruktur aufbaut, die zum Betreiben von verschiedenen KI-Lösungen benötigt aber nur selten voll ausgelastet wird. Vielmehr werden gewisse Prozesse teilweise „on-the-edge“ bei dem Leistungserbringern und anderen in Cloudumgebungen umgesetzt. Aufbauend auf einer sicheren Cloud-Umgebung, welche die in Kapitel 3 *Datenverarbeitung in der Cloud* erwähnten Anforderungen umsetzt, können verschiedene digitale Gesundheitsanwendungen isoliert voneinander betrieben werden. Basierend auf einem geeigneten und transparenten Einwilligungsmanagement können diese Anwendungen von verschiedenen Parteien wie Patienten, Pflegende und Behandelnde genutzt werden.

Mit geeigneten Verfahren zur Anonymisierung, einer passenden sicheren Systembasis und geeigneten Policies, wie Zugriffskontrolle, kann auch eine vertrauenswürdige anonymisierte Datenbasis geschaffen werden, die von Dritten wie Forschenden oder KMUs genutzt werden kann.

4. Ausblick und Fazit

Der bevorstehende Digitalisierungsschub im Gesundheitswesen wird dafür sorgen, dass die Möglichkeiten, die Patienten zu heilen erhöht und die Prozesse in den Krankenhäusern optimiert werden. Somit ist diese unabdingbar und wird die nächsten großen Innovationen in der Medizin ermöglichen. Allerdings werden sich prinzipiell die Risiken für einen Angriff auf die Krankenhaus IT auch erhöhen, da die Angriffsfläche wächst. Diese potenziellen Risiken müssen durch geeignete Cyber-Sicherheitsmechanismen reduziert werden, da in Krankhäusern, neben dem finanziellen Schaden auch die Unversehrtheit von Menschen auf dem Spiel steht. Die zu ergreifenden IT-Sicherheitsmaßnahmen sind einerseits organisatorischer Art, wie Awareness-Schulung von Mitarbeitern, aber andererseits sind insbesondere auch innovative IT-Sicherheitstechnologien nötig, die ein geeignetes Sicherheitslevel garantieren können. Gleichzeitig ist unabdingbar, dass im Falle eines temporären IT-Sicherheitsproblems die medizinischen Geräte weiter funktionieren bzw. nur isolierte Bereiche betroffen sind.

Nur ein ganzheitliches Konzept, dass IT-Sicherheit, Transparenz und Privatheit umsetzt wird das Vertrauen der Bürger:innen gewinnen, das diese neuartigen Anwendungen akzeptieren. Dieser Trend hat sich zuletzt in den Akzeptanzquote der verschiedenen „Corona Warn Apps“ gezeigt: In Ländern in denen Datenschutz und IT-Sicherheit zentraler Bestandteil des Konzepts sind, wurde diese deutlich besser angenommen. So wurde die „deutsche” Warn-App des Robert Koch Instituts von 22 % der Bevölkerung installiert, wohingegen das französische Pendant, dass auf zentraler Datenhaltung basiert, nur von 4 % der Bevölkerung genutzt wird (Welt, 2020).

5. Literatur

(Heise online, 2016) Heise online (2016) US-Krankenhaus: 5,5 Millionen US-Dollar Strafe wegen Datenverlust https://www.heise.de/newsticker/meldung/US-Krankenhaus-5-5-Millionen-US-Dollar-Strafe-wegen-Datenverlust-3289330.html (abgerufen am 22. Oktober 2020)

(Pohlmann, 2019) Pohlmann N (2019) Cyber-Sicherheit - Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. Springer Vieweg Verlag, Wiesbaden

(Frost & Sullivan, 2019) Frost & Sullivan (2019) Medical Device and Network Security -- Coming to terms with the Internet of Medical Things (IoMT)

(gematik, 2020) gematik (2020) Arena für digitale Medizin – Whitepaper Telematikinfrastruktur 2.0 für ein föderalistisch vernetztes Gesundheitssystem

(Welt, 2020) Welt (2020) Wo Corona-Apps in Europa bisher gescheitert sind. URL: https://www.welt.de/politik/ausland/article216351558/Corona-App-in-Europa-Wo-sie-gescheitert-ist-und-wo-nicht.html (abgerufen am 22. Oktober 2020)

(Sabt, 2015) Mohamed Sabt, Mohammed Achemlal, Abdelmadjid Bouabdallah. (2015) Trusted Execution Environment: What It is, and What It is Not. 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications

Norbert Pohlmann ist Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco. Im Sommersemester 2013 war er als Gastprofessor an der Stanford University im Fachbereich Computer Science, Silicon Valley, USA. Die vielfältigen Fachartikel sowie mehrere Lehr- und Sachbücher auf dem Gebiet der Cyber-Sicherheit dokumentieren seine Passion für das Gebiet und machen ihn zu einem nachgefragten Experten für Interviews und Diskussionen.

Dr. **Tobias Urban** arbeitet als Postdoktorand im Institut für Internet-Sicherheit und als Berater bei der secunet Security Networks AG. Im Allgemeinen befasst er sich mit Themen, die Vertrauen und Transparenz in einer Digitalen Welt schaffen, erhöhen und festigen. Sein aktueller Fokus liegt auch Technologien, die Sicherheit und Privatsphäre im Web erhöhen.