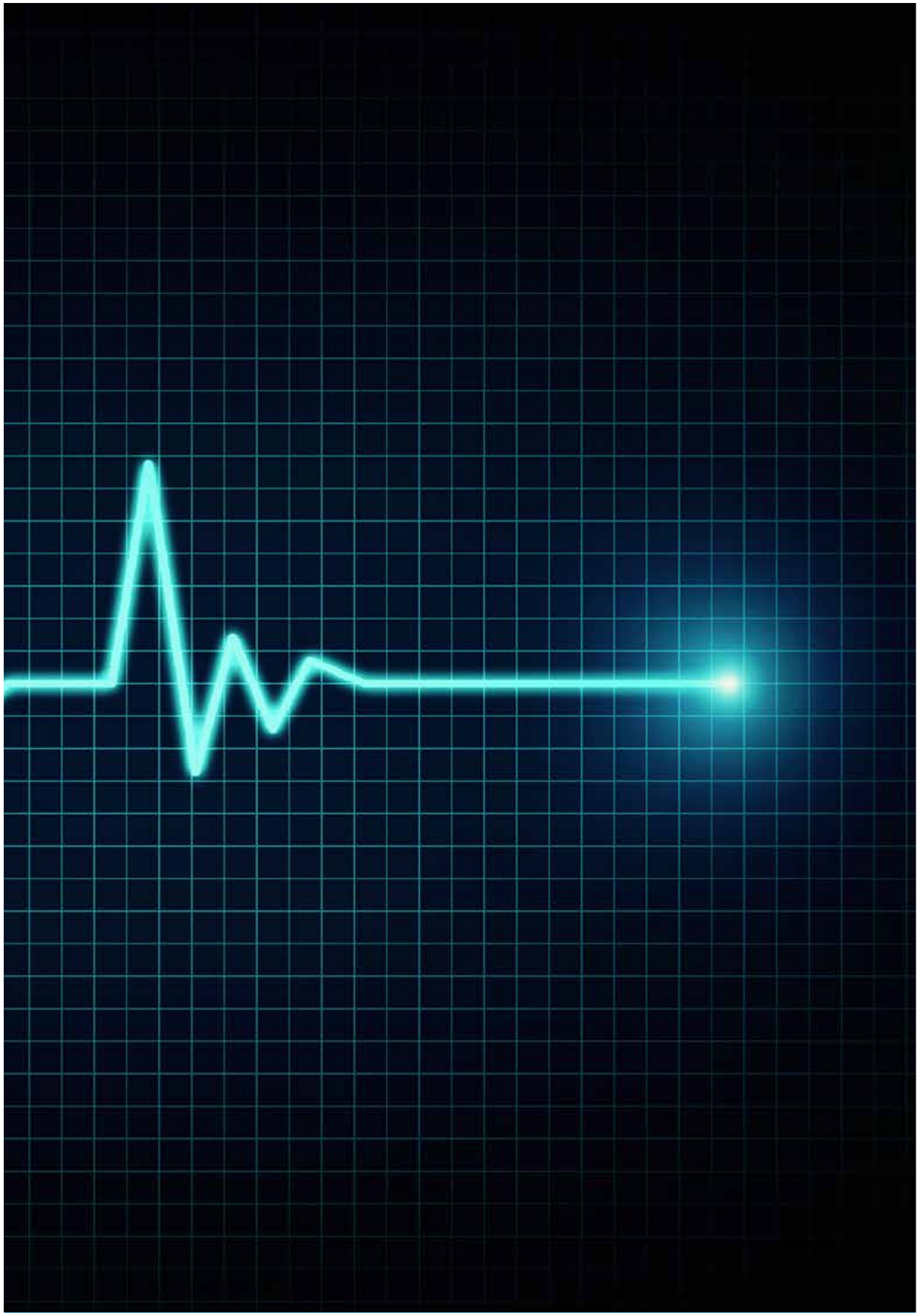
Tätigkeits-bericht Gesundheit

Cybersicherheit im Gesundheitswesen 2023

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•



Inhalt

1. Einleitung

Der vorliegende „Tätigkeitsbericht Gesundheit 2023“ stellt die Aktivitäten des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Bereich der sicheren Digitalisierung des Gesundheitswesens dar. Der Bericht deckt ein weites Spektrum ab: Beginnend mit den gesetzlichen Aufgaben des BSI im Bereich der Fortentwicklung der Telematikinfrastruktur (TI) leitet er über zur Sicherheit in der ambulanten Versorgung, um anschließend einen Überblick über die BSI-Aktivitäten im Bereich der Medizintechnik zu geben. Explizit nicht Thema dieses Berichts sind Aspekte der Kritischen Infrastrukturen.

Im Berichtszeitraum galt es, in allen benannten Bereichen zahlreichen Herausforderungen zu begegnen. In der Telematikinfrastruktur schritten die Aktivitäten zum Umbau der Infrastruktur vom geschlossenen VPN hin zu einem Zero-Trust-System (TI 2.0) fort. Begleitet wurde und wird eine solche Umgestaltung durch den Einsatz von Brückentechnologien, beispielsweise dem Highspeed-Konnektor, der Dienste wie „Konnektor-as-a-Service“ oder das TI-Gateway ermöglicht. Diese Technologie erleichtert den Leistungserbringer-Institutionen den Übergang von der aktuellen TI zu einer TI 2.0.

Parallel zu solch infrastrukturellen Aktivitäten, bei denen das BSI der TI gewissermaßen unter die Motorhaube schaute, stellte die Entscheidung des Gesetzgebers zur Realisierung einer sogenannten „Opt-Out-ePA“ oder „elektronischen Patientenakte für alle (ePA4all)“ das BSI gemeinsam mit der Nationalen Agentur für Digitale Medizin (gematik) vor eine weitere Aufgabe: Die hohen Sicherheitsziele der bisherigen, bereits realisierten elektronischen Patientenakte mussten auf die neue Architektur übertragen werden, sodass auch diese ein angemessenes Sicherheitsniveau erreicht.

Eine besondere Bedeutung kam im Jahr 2023 dem Bereich der ambulanten Versorgung zu. Das BSI beleuchtete mit zwei Projekten die Sicherheit in den Arztpraxen Deutschlands. Zum einen durch eine fokussierte Einzelbetrachtung innerhalb des Projekts „CyberPraxMed“ und zum anderen mit einer Umfrage unter mehr als 1.500 Ärztinnen und Ärzten, die gebeten wurden, eine Selbsteinschätzung der Cybersicherheit innerhalb ihrer Praxis anhand eines standardisierten Online-Fragebogens abzugeben. Die Ergebnisse zeigten dem BSI, dass auch im Jahr 2024 noch ein großer Bedarf für die Erhöhung der Sicherheit in Arztpraxen gegeben ist.

Die Bewertung schwerwiegender Sicherheitsvorfälle bei Medizinprodukten ist eine spezialgesetzliche Aufgabe des BSI. Präventiv ist das BSI hier mit dem Festlegen von Sicherheitsanforderungen befasst. Im Jahr 2023 standen dabei die Digitalen Gesundheits- und Pflegeanwendungen im Fokus.

Die folgenden Kapitel stellen eine Auswahl an BSI-Aktivitäten für das Gesundheitswesen im Jahr 2023 detailliert dar, mit denen die Cybersicherheit in diesem Sektor pragmatisch erhöht werden kann.

2. Digitalisierungs-bereiche

2.1 Telematikinfrastruktur

Aktuelle Entwicklungen der Telematikinfrastruktur

Die Telematikinfrastruktur (TI) ist die deutsche Plattform zur Vernetzung aller Beteiligten im Gesundheitswesen. Seit Ihrer Anfangszeit, die sich vor allem auf Basisfunktionalitäten, wie eine elektronische Gesundheitskarte oder Versichertenstammdaten-Management, konzentrierte, unterlag sie immer wieder tiefgreifenden Erneuerungen durch zusätzliche Anforderungen und Möglichkeiten. Auch nun stehen tiefe Anpassungen der Architektur bevor, um die TI an die neuen Ziele des Gesundheitsdatennutzungsgesetzes (GDNG) und des Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (DigiG) anzupassen. Zugleich werden die durch die TI ermöglichten Anwendungen fortlaufend erweitert und verbessert.

Modernisierungen durch DigiG und GDNG

Durch das Gesundheitsdatennutzungsgesetz (GDNG) erhalten Forschende die Möglichkeit, anonymisierte Gesundheitsdaten für Gemeinwohlzwecke leichter zu nutzen.[1] Über eine zentrale Datenzugangs- und Koordinierungsstelle können Daten genutzt und auch Daten aus unterschiedlichen Quellen miteinander verknüpft werden. Hierfür sind unter anderem Anpassungen im Rahmen der unten als Fokusthema betrachteten „ePA4All“ erforderlich. Zum Schutz der Gesundheit von Versicherten sollen auch Kranken- und Pflegekassen Patientendaten verarbeiten dürfen.

Zugleich soll die Gestaltung der Digitalisierung des Gesundheitswesens mit dem Digital-Gesetz (DigiG)[2] durch eine veränderte Rollenverteilung beschleunigt werden. Mit dem BSI und dem Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) soll zukünftig kein Einvernehmen zu Fragen der IT-Sicherheit und des Datenschutzes mehr erforderlich sein, sondern es soll eine Beratung innerhalb eines neuen Digitalbeirats erfolgen, in dem die beiden Behörden vertreten sind. Die Aspekte der IT-Sicherheit und des Datenschutzes verlagern sich somit wesentlich stärker auf die gematik – die auch jetzt schon letztendlich die Verantwortung für Risiken trägt – und infolgedessen auf die dort vorgesehenen Zulassungsverfahren. Dem BSI hingegen bietet sich dadurch die Möglichkeit, sich gestaltend am Design der IT-Sicherheit zu beteiligen, jedoch wird das BSI keinen direkten Einfluss auf Risikomitigation oder Risikoakzeptanz haben. In diesem Rahmen entfällt auch die gesetzliche Pflicht zu einer Zertifizierung von Komponenten und Diensten nach Prüfvorgaben des BSI, sofern diese nicht nach Ermessen der gematik als Risiko-Owner als Teil des Zulassungsverfahrens vorgesehen sind.

Durch das DigiG erhalten auch private Krankenversicherungen die Möglichkeit, eine Opt-out-ePA (ePA4all) anzubieten. Gesetzliche Krankenkassen müssen also eine ePA anbieten, der ein Versicherter auf eigenen Wunsch aktiv widersprechen darf, und diese Möglichkeit steht nun auch privaten Krankenkassen offen. Ferner sollen bestehende Anwendungsfälle verbessert werden: So wurde das E-Rezept ab 01.01.2024 als verbindlicher Standard in der Arzneimittelversorgung etabliert und stark vereinfacht. Während der klassische elektronische Medikamentenplan den früheren papiergebundenen Medikamentenplan digital nachbildete, soll eine neue digitale Medikationsübersicht auf Grundlage der ePA dem Versicherten eine weitgehend automatisierte Übersicht liefern , was insbesondere bei vielen Medikamenten oder Patienten mit wenig medizinischem Wissen die Behandlung erleichtern kann. Auch die Integration von Digitalen Gesundheits- und Pflegeanwendungen (DiGA und DiPA, siehe auch Abschnitt 2.3.4), Telemonitoring und Telemedizin soll verbessert werden, sodass die Digitalisierung des Gesundheitswesens nicht mehr als Zusammenstellung von Insellösungen wahrgenommen wird, sondern zu einem gemeinsamen Versorgungsportfolio zusammenwächst.

Fokusthemen

Ausgewählte aktuelle Themen der Telematikinfrastruktur werden in den folgenden Abschnitten kurz erläutert und in den nächsten Unterkapiteln im Detail beleuchtet.

Im Rahmen der Zero-Trust-Architektur beleuchtet Abschnitt 2.1.1 den Wandel der TI von einer auf Leistungserbringer fokussierten geschlossenen Umgebung hin zu einer Architektur, die für Anwendungen der Patientinnen und Patienten und anderer Akteure geöffnet ist und auf die zusätzlich mit herkömmlichen Geräten wie Smartphones anstatt Konnektoren zugegriffen werden kann. Statt einer rein auf Hardware basierenden Sicherheit soll vermehrt auch auf Digitale Identitäten gesetzt werden.

Durch die „ePA4All“ sollen die Versorgungsprozesse optimiert werden, indem Patientinnen und Patienten per Opt-Out standardmäßig eine Patientenakte angelegt bekommen, die von behandelnden Ärztinnen und Ärzten und anderen Leistungserbringern befüllt werden kann. Der Patient kann dieser Akte widersprechen oder die Zugriffsmöglichkeiten einschränken. Durch dieses neue Paradigma ändern sich die Anforderungen an die IT-Sicherheit. Es werden Zugriffe auf die Patientenakte ohne aktive Einwilligung des Patienten erforderlich, die aber weiterhin geeignet abgesichert sein müssen. Diese Neuausrichtung wird in Abschnitt 2.1.2 genauer beleuchtet.

In der derzeit bestehenden Architektur der TI stellt der Konnektor einen wesentlichen Bestandteil des sicheren Netzzuganges für Ärztinnen und Ärzte und andere Leistungserbringer dar. Der in Abschnitt 2.1.3 beschriebene Highspeed-Konnektor verbessert diesen Netzzugang für große Einrichtungen wie Krankenhäuser, indem die Funktionalität vieler Konnektoren gebündelt wird.

2.1.1 Zero Trust

Im Zuge der Digitalisierung im Gesundheitswesen wird angestrebt, immer mehr Anwendungsfälle in die Telematikinfrastruktur (TI) zu verlagern. Für die Versicherten ist es beispielsweise möglich, mit dem Smartphone auf die elektronische Patientenakte zuzugreifen und elektronische Rezepte einzulösen. Zudem sollen Ärztinnen und Ärzte auch von außerhalb der Praxisumgebung Einsicht in die Akten ihrer Patientinnen und Patienten haben.

Die Architektur der Telematikinfrastruktur 1.0 basiert auf einer per Smartcard und sicherer Hardware realisierten Ende-zu-Ende-Verschlüsselung und läuft innerhalb eines virtuellen privaten Netzwerks (VPN). Der Zugang zu diesem Perimeter-basierten Netzwerk war ursprünglich nur für die Leistungserbringer (LE), wie z. B. Arztpraxen und Krankenhäuser, angedacht. Hierzu wurde eigens für die TI 1.0 der Konnektor entwickelt, ein spezieller Router, welcher dem Leistungserbringer den Zugang zur Telematikinfrastruktur ermöglicht. Die Identifizierung der Teilnehmenden ist dabei hardwarebasiert und größtenteils über Chipkarten realisiert.

Durch die fortschreitende Digitalisierung im Gesundheitswesen, die intensivere Nutzung von mobilen Endgeräten und den Trend, beim Zugriff auf Gesundheitsdaten nicht an einen bestimmten Ort sowie Zeitpunkt gebunden zu sein, wächst die Zahl der Teilnehmenden und der teilnehmenden Geräte in der Telematikinfrastruktur. Die Architektur der TI 1.0, mit dem Konnektor als Zugangspunkt, ist dafür nicht ausgelegt. Der Konnektor ist sicherheitszertifiziert und eigens für die Telematikinfrastruktur entwickelt worden. Dadurch verfügt die Telematikinfrastruktur zwar über ein hohes Maß an Sicherheit, das Aktualisieren der bestehenden Komponenten sowie das Einbringen von neuen Komponenten ist dadurch jedoch sehr aufwendig.

Um die Telematikinfrastruktur an die neuen Herausforderungen der Digitalisierung des Gesundheitswesens anzupassen, wurde ein Paradigmenwechsel beschlossen. Die Architektur der TI 1.0 soll grundlegend verändert werden. Es ist geplant, den Zugang über den Konnektor und damit einer wesentlichen Komponente des Perimeterschutzes in der neuen TI 2.0 entfallen zu lassen.

Für die neue Architektur der Telematikinfrastruktur wurde ein Zero-Trust-Ansatz gewählt. Zero Trust basiert grundsätzlich auf dem Prinzip der minimalen Rechte aller Nutzenden, Geräte und Systeme. Bei dieser Betrachtung wird die Idee eines sicheren internen Netzes hinterfragt . Eine mögliche Folge davon ist, dass man z. B. bei der Absicherung eines Service die Annahme trifft, dass dieser für den Angreifer bereits erreichbar ist. Für den Zugriff auf die TI 2.0 müssen Anfragende deshalb ein messbares Sicherheits- und Vertrauensniveau nachweisen. Dies soll neben der Stärke der Authentisierung auch Informationen über den Sicherheitsstatus des verwendeten Endgerätes, Metadaten der Verbindung und weitere Informationsquellen berücksichtigen. Diese eingelieferten Informationen werden dann gegen zuvor fest definierte Zugriffsrichtlinien abgeglichen, die so eine individuelle Zugriffsentscheidung auf Basis dynamischer Informationen ermöglichen.

Die Zero-Trust-Architektur für die Telematikinfrastruktur 2.0 soll es ermöglichen, mit aktuell verfügbaren Smartphones an der TI 2.0 teilzunehmen. Dafür ist es erforderlich, den Zugriff auf die TI 2.0 erst nach Prüfung von Sicherheitszustand und Schutzmaßnahmen des verwendeten Endgeräts zu ermöglichen. Die Architektur sieht ein Regelwerk auf der Basis von Attribute-Based Access Control vor. Dabei können bei der Zugriffsentscheidung Attribute berücksichtigt werden, welche dynamisch zum Zeitpunkt der Zugriffsanfrage erhoben werden. So könnten beispielsweise Zugriffe von auffälligen IP-Adressbereichen oder von Geräten, die nicht über aktuelle Sicherheitsupdates verfügen, blockiert werden. Weiterhin ist es vorstellbar, dass Versicherte eigene Zugriffsregeln definieren können und damit z. B. Zugriffe aus bestimmten Ländern

oder zu bestimmten Zeitpunkten, je nach persönlichem Bedarf, unterbunden werden können. Anstatt auf Spezialanfertigungen soll vermehrt auf Standards gesetzt werden, um bei technischen Weiterentwicklungen schneller reagieren zu können.

Ganz allgemein steht bei Zero Trust die Integrität und die Vertraulichkeit im Fokus und nicht die Verfügbarkeit. Diese ist im Gesundheitswesen aber von zentraler Bedeutung. Daher ist vorgesehen, die Komponenten redundant auszulegen und die Kommunikation weitgehend statuslos ablaufen zu lassen, sodass Ausfälle kompensiert werden können.

Mit Hilfe der Zero-Trust-Architektur für die Telematikinfrastruktur sollen durch den Verzicht auf spezielle Zugangshardware die Kosten gesenkt werden[3]. Allerdings ist eine ganzheitliche, wirksame Umsetzung von Zero-Trust-Prinzipien ein langfristiges Vorhaben und erfordert einen ebenso hohen wie dauerhaften finanziellen sowie personellen Ressourcenaufwand[4].

Die Feststellung der Konformität von privaten Endgeräten, aber auch von Endgeräten in Leistungserbringerumgebungen, ist aus Sicht der TI 2.0 eine zentrale Herausforderung der Zero-Trust-Architektur. Mit der fortlaufenden Digitalisierung im Gesundheitswesen und damit der Verlagerung von immer mehr Prozessen in die Telematikinfrastruktur erhöhen sich jedoch die Angriffsoberfläche und das Schadenspotenzial. Das BSI begleitet daher als beratende Instanz den Entwicklungsprozess, sichtet, bewertet und kommentiert Konzeptpapiere und prüft permanent, ob die angestrebte Architektur in Bezug auf die IT-Sicherheit realisierbar ist.

2.1.2 Die elektronische Patientenakte für alle

Durch die Einführung der elektronischen Patientenakte für alle (ePA4all) ab 2025 soll der Digitalisierungsgrad innerhalb der Versorgung im deutschen Gesundheitswesen deutlich ausgebaut werden.

Derzeit existiert die elektronische Patientenakte (ePA 2.6) auf Basis einer so genannten Opt-In-Variante. Dies bedeutet, dass jeder Versicherte auf Wunsch und allein durch eigeninitiatives Vorgehen eine solche elektronische Akte bei seiner gesetzlichen Krankenkasse beantragen kann. Zudem müssen Versicherte jeden einzelnen Leistungserbringer aktiv für den Zugriff auf die persönliche elektronische Akte berechtigen.

Die neu geplante ePA4all hingegen beschreibt durch den Opt-Out-Ansatz einen deutlichen Fokuswechsel. Im Rahmen des Opt-Out-Verfahrens wird für jeden gesetzlich Versicherten eine elektronische Patientenakte automatisch durch den Versicherer angelegt. Ziel dieses neuen Vorgehens ist der Wechsel von einer rein versichertenzentrierten Dokumentenablage hin zur Verbesserung der digitalen Versorgungsprozesse für Leistungserbringer und Versicherte. Dies schafft eine nachhaltige Basis für eine moderne Behandlung und die Forschung im Gesundheitswesen.

Durch einen strukturierten und standardisierten Austausch der Gesundheitsdaten wird ein effizienter und durchgängiger Versorgungsprozess gestärkt und sichergestellt. Darüber hinaus vereint die neue ePA4all weitere Vorteile für die Nutzerinnen und Nutzer. Neben rein praktischen Anwendungsindikationen, beispielsweise dem vereinfachten Suchen und Filtern von Daten und Dokumenten, ermöglicht die ePA4all eine lückenlose Datenverarbeitung und Datenverfügbarkeit im Falle eines Krankenkassenwechsels. Die Nutzung der ePA4all ist zudem auch ohne die entsprechende ePA-App möglich.

Durch die Umstellung auf eine Opt-Out-Akte ergeben sich im Rahmen der Architektur der ePA deutliche Veränderungen und daraus resultierend veränderte Sicherheitsanforderungen, um ein angemessenes Schutzniveau für die ePA sicherzustellen.

Der technische Fokus der neuen Sicherheitsarchitektur liegt auf der sicheren Dokumentenverarbeitung und Datenkommunikation, nicht mehr ausschließlich auf der Dokumentenablage. Um auszuschließen, dass der Betreiber der Aktensysteme Einsicht in die abgelegten Daten und Dokumente erhält, werden auch bei der neuen Sicherheitsarchitektur der ePA4all eine Reihe von Maßnahmen ergriffen. So werden verschiedene hardware- und softwarebasierte Mechanismen etabliert und durch organisatorische Konzepte ergänzt. Die Vertrauenswürdige Ausführungsumgebung (VAU) schützt auf technischer Ebene sowohl die medizinischen Metadaten als auch die Dokumente während der Verarbeitung. Dies gewährleistet ein angemessenes Sicherheitsniveau für den Schutz der medizinischen Daten, während sie im Aktensystem verarbeitet werden. Bei der tatsächlichen Ablage und Speicherung werden medizinische Informationen verschlüsselt. Ein ähnlicher Mechanismus wird derzeit schon beim eRezept angewendet.

Durch das neue Digitalgesetz (DigiG) soll der Prozess mit Blick auf die Erneuerung der ePA erheblich beschleunigt werden. Die Zuständigkeit für die Entwicklung der Architektur sowie der Implementierung der ePA liegen in der Hand der gematik. Diese vertritt die technisch-fachliche Anforderungslage, welche den Rahmen für die Umsetzung durch die Krankenkassen bildet. Das BSI steht der gematik in Hinblick auf die IT-Sicherheit der ePA4all durch die Wandlung von der Einvernehmens- zur Benehmensregelung beratend zur Seite. Alle Beteiligten arbeiten gemeinsam daran, eine funktionale, benutzerfreundliche und angemessen sichere Lösung zu schaffen, um mit der ePA4all die Gesundheitsversorgung in Deutschland durchgängiger und moderner zu gestalten.

2.1.3 Der Highspeed-Konnektor

Konnektoren bilden heute einen wesentlichen Bestandteil der dezentralen Telematikinfrastruktur (TI). Es handelt sich hierbei um sichere Komponenten, die den (Netz-)Zugang zur Telematikinfrastruktur für Leistungserbringer und weitere Zugriffsberechtigte ermöglichen. Der Konnektor übernimmt eine gesicherte Verbindung zum VPN-Zugangsdienst der Telematikinfrastruktur. Umgangssprachlich wird ein klassischer Konnektor auch Einbox-Konnektor genannt.

Diese klassischen Konnektoren sind Hardwarekomponenten, die vor Ort in Krankenhäusern und Praxen installiert und i. d. R. von einem „Dienstleister vor Ort“ betreut werden.

Vor dem Hintergrund der Modernisierung der Telematikinfrastruktur und der damit verbundenen Ausrichtung am Bedarf der Anwendenden wurden die sogenannten „Highspeed-Konnektoren“ durch die gematik spezifiziert.

Der Highspeed-Konnektor kann die Funktion der Konnektoren für große Institutionen (wie Krankenhäuser) übernehmen. Aktuell müssen solche Institutionen eine Vielzahl von Einbox-Konnektoren betreiben und haben ein Bedürfnis nach einer performanteren und einfacher zu verwaltenden Lösung.

Die Highspeed-Konnektoren werden im Rahmen einer Beschleunigten Sicherheitszertifizierung (BSZ) durch das BSI zertifiziert. Bisher konnte ein Anbieter die Zertifizierung erfolgreich durchlaufen.

Die BSZ ermöglicht es Herstellern, ihre Sicherheitsaussagen bezüglich eines Produktes durch ein unabhängiges Zertifikat bestätigen zu lassen. Das zugehörige Zertifizierungsschema basiert auf planbaren Evaluierungslaufzeiten und hält den Aufwand für den Produkthersteller – insbesondere im Bereich der Dokumentation – überschaubar. Die Evaluierung folgt einem risikogetriebenen Ansatz, der ein hohes Niveau an Vertrauen in die Sicherheitsaussagen schafft.[5]

Eine nachgelagerte Ausbaustufe eines Highspeed-Konnektors stellt das TI-Gateway dar. Im Kern besteht das TI-Gateway aus einem Highspeed-Konnektor und einem Zugangsmodul. Das Zugangsmodul ermöglicht die Nutzung des Highspeed-Konnektors durch mehrere Mandanten, indem es die komplexe, rollenbasierte Steuerung von Zugängen zum Highspeed-Konnektor regelt und den Zugang aus der Ferne etabliert. Das TI-Gateway kann also von mehreren, unterschiedlichen Leistungserbringern genutzt werden: „Es eröffnet die Möglichkeit, dass ein einzelner Highspeed-Konnektor in einem sicheren Rechenzentrum eine Vielzahl an Praxen sicher und mit entsprechenden Supportleistungen an die TI anbinden kann. Die Installation eines einzelnen Konnektors vor Ort in der Praxis ist damit nicht mehr notwendig.[6] “Das TI-Gateway schafft eine solide Spezifikationsbasis für Betreibermodelle wie etwa ein geregeltes „Konnektor-as-a-Service“-Angebot.

Voraussetzung für die Bereitstellung eines TI-Gateway wird eine Anbieterzulassung durch die gematik sein. Um den Dienst Leistungserbringern anbieten zu können, ist die vorherige Zulassung unabdingbar.

2.2 Ambulante Versorgung

2.2.1 Ausgangslage

Das Sozialgesetzbuch fünf (SGB V) definiert für das BSI unterschiedliche spezielle Aufgaben im Gesundheitswesen. Die bekannteste spezielle Zuständigkeit ist mit den Tätigkeiten im Kontext der Telematikinfrastruktur in Kapitel 2.1 bereits erwähnt worden. Leistungserbringer können auf eine stetig steigende Vielzahl unterschiedlicher Anwendungen zugreifen und diese nutzen, auch solche, die auf der Telematikinfrastruktur aufbauen. Neue Anwendungen sind die umfangreichere Verwendung der elektronischen Patientenakte (ePA), das elektronische Rezept (eRezept) oder auch die direkte Kommunikation mit anderen Praxen via Kommunikation im Medizinwesen (KIM). Diese und weitere digitale Angebote werden zunehmend in den Praxisalltag integriert. Die Anwendungen haben zum Ziel, die gesundheitliche Versorgung zu optimieren, doch bleibt eine Komplexitätssteigerung in der jeweiligen IT-Landschaft durch diese Ergänzungen unvermeidbar. Durch die relevante Rolle innerhalb der Versorgung bestehen unvermeidbare Abhängigkeiten von einer funktionierenden IT.

Das BSI betrachtet im Kontext des Gesundheitswesens nicht nur die Cybersicherheit der Anwendungen für das Gesundheitswesen, sondern auch die IT-Sicherheit und Cybersicherheit in den Nutzungsumgebungen eben dieser Anwendungen. Konkret betrachtet das BSI hierbei die IT-Sicherheit in den Arzt- und Zahnarztpraxen und wird von der Kassenärztlichen Bundesvereinigung (KBV) und der Kassenzahnärztlichen Bundesvereinigung (KZBV) bei der Erstellung der IT-Sicherheitsrichtlinie gem. § 75b SGB V im Einvernehmen beteiligt.

Die 2020 erstmals veröffentlichte Richtlinie soll den Praxisbetreiben dazu dienen, ein ausreichendes Sicherheitsniveau einzuhalten. Die grundlegenden Maßnahmen in der Richtlinie widmen sich beispielsweise dem grundsätzlichen Umgang mit Gesundheitsdaten durch Berücksichtigung einer konsequent verschlüsselten Kommunikation und Aufbewahrung. Um ein ausreichendes Sicherheitsniveau zu erreichen, ist es unerlässlich, den Überblick über die zum Teil vielseitige IT-Landschaft zu behalten und gezielt präventive Maßnahmen zu etablieren. Essentiell ist dabei die Erstellung eines Netzwerkplanes. Dieser Netzwerkplan, in Kombination mit vorab abgestimmten Verhaltensweisen und erlernten und erprobten Handlungsweisen des Praxispersonals, sorgt dafür, dass Ausfälle schneller behoben werden können und nachfolgend die reibungslose IT-gestützte Versorgung frühzeitiger wiederaufgenommen werden kann. Die Maßnahmen und Anforderungen, die die KBV, die KZBV und das BSI veröffentlicht haben, zielen darauf ab, erste Schritte für einen grundlegenden Schutz umzusetzen. Jedoch kann nicht davon ausgegangen werden, dass die über 100.000 Arztpraxen in Deutschland jederzeit von einem Angriff verschont bleiben. Aus diesem Grund ist auch die Resilienz der IT in den unterschiedlichen Praxen wichtig. Darüber hinaus ermöglicht die Richtlinie eine stetige Neubewertung der Bedrohungslage und der dazu passenden Schutzmaßnahmen, um ein ausreichendes Schutzniveau zu etablieren.

2.2.2 Cybersicherheit in Arztpraxen (CyberPraxMed)

Im Zeitraum von Ende 2022 bis Ende 2023 wurde durch das BSI das Projekt CyberPraxMed durchgeführt, in dessen Rahmen die Cybersicherheit in Arztpraxen untersucht wurde. Dabei sollten insbesondere Angriffsmöglichkeiten erörtert werden, die sich aufgrund der Netzwerkstruktur, des Personals und trotz eventuell bereits vorhandener Sicherheitsvorkehrungen bieten. Dazu wurde ein Fragebogen erstellt und auf dessen Basis wurden 16 ausgewählte Arztpraxen per Videokonferenz im Beisein eines eventuell vorhandenen IT-Dienstleisters befragt. Die Auswahl der Arztpraxen erfolgte nach den Kriterien „Fachgebiet“ (allgemeinmedizinische Praxen, Zahnarztpraxen, psychotherapeutische Praxen und radiologische Praxen), „Anzahl der Mitarbeiterinnen und Mitarbeiter“ (1 – 150) sowie „geographische Lage“ (ländliche und städtische Lage). Zudem sollte die Relevanz des jeweiligen Kriteriums im Verhältnis zur Anzahl der Schwachstellen erfasst werden. Als Projektziel wurde ein Projektbericht über die gegenwärtige Sicherheitslage verfasst, der Schwachstellen zusammen mit einer Risikobewertung und Handlungsempfehlungen auflistet. Darüber hinaus wurde eine kompakte Liste mit Empfehlungen erarbeitet, die Ärztinnen und Ärzten die Möglichkeit bietet, ihre Praxen mit möglichst geringem Aufwand robuster gegen Cyberangriffe zu machen.

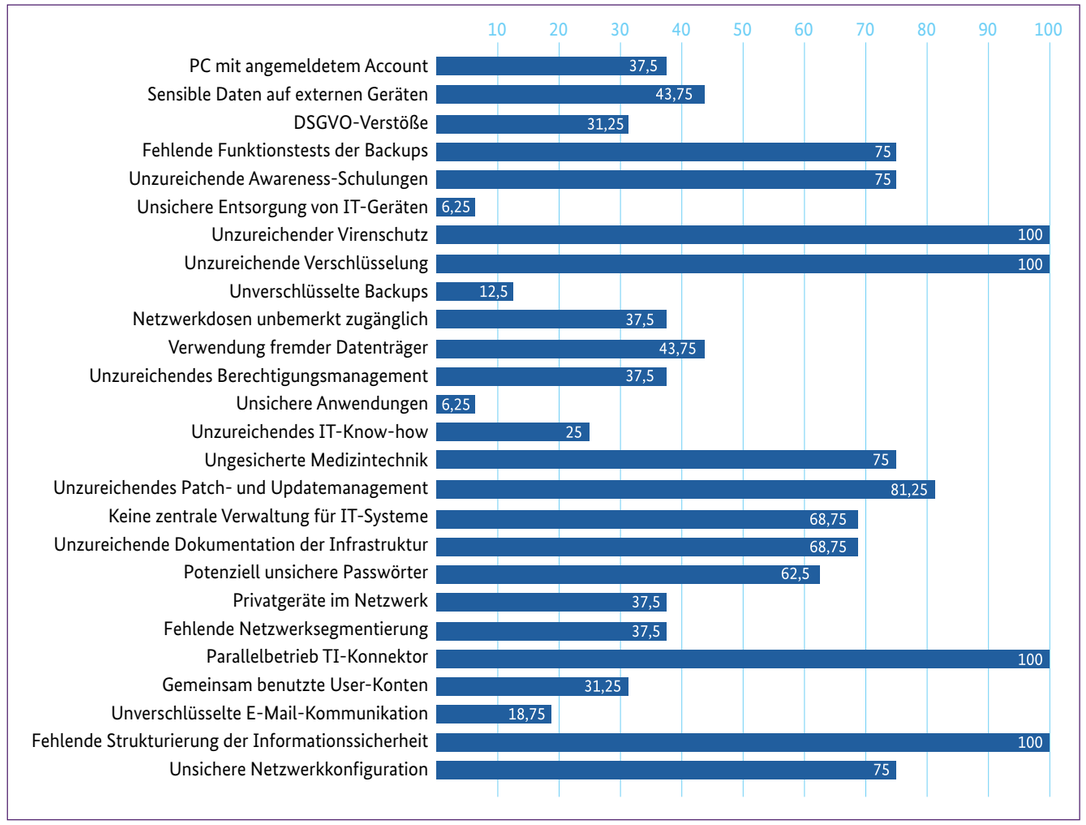
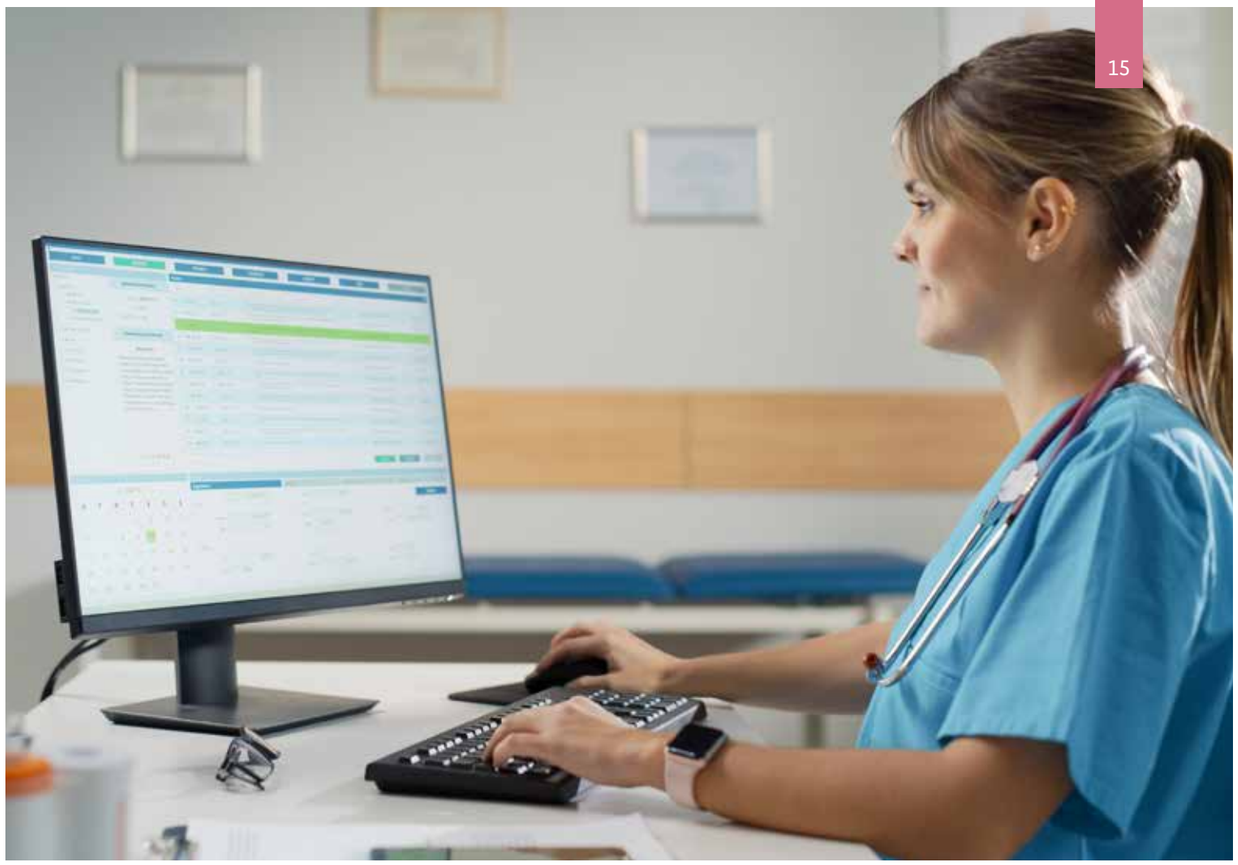


Abbildung 1 – Häufigkeit der Schwachstellen in Prozent



Die in Abbildung 1 dargestellten Ergebnisse des Projekts zeigen, dass es einige Schwachstellen gibt, die den Großteil oder sogar alle befragten Praxen betreffen. Davon abgesehen, dass keine der Praxen über ein sogenanntes ISMS (Information Security Management System) verfügt, das Regeln und Verfahren zur Gewährleistung der Cybersicherheit festlegt, konnte in keiner Praxis ein ausreichender Schutz vor Schadsoftware festgestellt werden. In keiner der befragten Praxen kam eine Festplattenverschlüsselung zur Sicherstellung einer hohen Datensicherheit zum Einsatz. Des Weiteren befand sich in allen Praxen der Konnektor zur Anbindung an die Telematikinfrastruktur im Parallelbetrieb zu einem gewöhnlichen Router und kann dadurch seine Schutzwirkung nicht vollständig entfalten. Zudem gab es in den meisten Praxen ein unzureichendes Patchmanagement und es war nicht gewährleistet, dass Backups funktionsfähig sind, die beispielsweise im Fall eines Ransomware-Angriffs essentiell sind. Vernetzte Medizinprodukte waren in fast allen Fällen nicht gesondert vor einer Manipulation gesichert. Es konnten keine nennenswerten Korrelationen zwischen den gefundenen Schwachstellen und der Praxisgröße, der Größe eines eventuell vorhandenen Dienstleisters und der geographischen Lage beobachtet werden. Die Datenbasis des Projekts ist allerdings zu klein, um belastbare Schlüsse zu ziehen.

Die Ergebnisse des Projekts CyberPraxMed bestätigen den Verdacht, dass der Großteil der befragten Arztpraxen, deren IT-Systeme per Definition kein Teil der Telematikinfrastruktur sind, einige verhältnismäßig einfach zu behebende Sicherheitsmängel aufweist. Die Projektergebnisse sind für das BSI als Stichprobe geeignet, um aufbauende Projekte zu planen. Zudem sollen die Ergebnisse als unmittelbare Folge Ärztinnen und Ärzte motivieren, einen kritischen Blick auf die Cybersicherheit in Praxen zu entwickeln und bereits zum jetzigen Zeitpunkt die gegebenen Handlungsempfehlungen umzusetzen. Sofern diese in einem Großteil der Praxen umgesetzt werden, kann die Sicherheit in einem bedeutenden Teil des Gesundheitswesens erhöht werden.

2.2.3 Evaluierung der IT-Sicherheitsrichtlinie in Arztpraxen (SiRiPrax)

Um die Digitalisierung im Gesundheitswesen weiter voranzutreiben, ist von der Bundesregierung das „Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation“ (Digitale-Versorgung-Gesetz, DVG) zum 19. Dezember 2019 in Kraft getreten. Im Zuge dieser Gesetzesnovellierung wurde das SGB V um § 75b, wie im Eingangskapitel bereits beschrieben, erweitert. Mit diesem Zusatz sollen künftig grundlegende Sicherheitsmaßnahmen für Arzt- und Zahnarztpraxen garantiert werden. Da die Verantwortung für die Einhaltung und Umsetzung dieser Maßnahmen bei den Praxisinhabenden liegt, ist die Verständlichkeit der Richtlinie und eine unkomplizierte Anwendbarkeit der Anforderungen maßgeblich.
Die IT-Sicherheitsrichtlinie wird jährlich hinsichtlich des Standes der Technik geprüft und an das aktuelle Gefährdungspotenzial angepasst. Um Einblicke in die bisherige Umsetzung und die Verständlichkeit der Richtlinie bei den Leistungserbringern zu erlangen, hat das BSI eine Befragung bei über 12.000 Arztpraxen deutschlandweit in Auftrag gegeben.

Dieses Vorhaben erfolgte im Rahmen des Projektes „Evaluierung der IT-Sicherheitsrichtlinie in Arztpraxen (SiRiPrax)“. Im Zeitraum von März bis Mai 2023 wurden 12.000 kleinere Arzt- und Zahnarztpraxen in ganz Deutschland angeschrieben, um an der BSI-Umfrage teilnehmen zu können. Besonderer Fokus lag hier zum einen auf der derzeitigen Umsetzung und Anwendbarkeit der IT-Sicherheitsrichtlinie nach § 75b SGB V sowie auf grundsätzlichen Parametern, die Aufschluss über die IT-Sicherheitslage in den teilnehmenden Praxen geben können. Beispielsweise widmen sich einzelne Fragestellungen der grundlegenden IT-Ausstattung, der Nutzung der IT und bestehenden digitalen Anwendungen für die Leistungserbringer.

Mit Rückmeldungen von rund 1.600 Arztpraxen zeigte sich ein hohes Interesse der Ärztinnen und Ärzte, das Thema IT-Sicherheit in den Praxen zu verbessern. Dieses Interesse wurde ebenfalls durch die Rolle der Teilnehmenden deutlich. Mit 79 % haben mehrheitlich Ärztinnen und Ärzte die Beantwortung des Fragebogens selber wahrgenommen. Die übrigen Befragten sind Praxismitarbeitende, vor allem medizinische Fachangestellte und Angestellte in der Verwaltung sowie im Praxis-Management. Bei lediglich einem Prozent der Praxen antworteten externe Dienstleister. Die meisten Befragten sind um die Sicherung und den Schutz ihrer Daten bemüht und halten sich bei diesem Thema für gut informiert. In fast jeder Praxis widmet sich ein IT-Sicherheitsbeauftragter der Thematik. Diese Zuständigkeit beeinflusst die IT-Sicherheit in der Praxis positiv. Jedoch ist hierbei eindeutig hervorzuheben, dass die verantwortlichen Personen in der Regel fachfremd sind und die Aufgaben im Bereich der IT-Sicherheit neben ihrer beruflichen Tätigkeit erledigen. Des Weiteren zeigt die Umfrage auf, dass das Thema und seine Bedeutung viele Praxen noch nicht erreicht hat, da die meisten Rückmeldungen eine eher geringe Bekanntheit der IT-Richtlinie nach § 75b SGB V und ihrer Umsetzung ergeben haben.

Die Anforderungen und Maßnahmen, die in der IT-Sicherheitsrichtlinie vorgegeben sind, sind derzeit nur in einem Drittel der Praxen vollumfänglich umgesetzt, obwohl es sich hierbei um gesetzliche Vorgaben handelt, die bis Juli 2022 hätten umgesetzt werden müssen. Die Antworten der Befragten verdeutlichen bestehende Umsetzungsprobleme der verantwortlichen Praxisinhabenden und Leistungserbringer. Zum einen bestehen Verständnisprobleme hinsichtlich der Vorgaben sowie grundsätzliche Zweifel am Nutzen der IT-Sicherheitsrichtlinie. Zum anderen mangelt es am Budget bei den Ärztinnen und Ärzten zur Ertüchtigung der jeweiligen IT-Infrastruktur, da Kosten, die durch die Realisierung einer effizienten IT-Sicherheit anfallen, eigenständig von der jeweiligen Praxis getragen werden müssen. Des Weiteren mangelt es an notwendigem Fachwissen sowie Zeit für die Umsetzung durch das Personal. Viele der befragten Praxen empfinden bei der Umsetzung der IT-Sicherheitsrichtlinie keine große Dringlichkeit, da sie meistens noch von keinem IT-Sicherheitsvorfall betroffen waren.
In den Praxen muss ein größeres Problembewusstsein für IT-Sicherheitsvorfälle geschaffen werden. Die IT-Sicherheitsrichtlinie muss allen Praxen bekannt gemacht und von allen umgesetzt werden. Um dies zu erreichen, sind die Anforderungen und Maßnahmen verständlich und anschaulich durch eine Kooperation des BSI mit den Stakeholdern des Gesundheitswesens zu vermitteln.

Mit Blick auf die IT-Ausstattung und deren Nutzung zeigt sich, dass die meisten Praxen Sicherheitsvorkehrungen getroffen haben. Fast jede Praxis legt beispielsweise regelmäßig sowohl automatisiert als auch manuell Sicherungskopien von wichtigen Daten an.

Gut zwei Drittel aller Praxen verschlüsseln ihre Daten regelmäßig, bevor diese lokal gespeichert oder versendet werden. Bei vier von zehn Praxen ist eine Datenverschlüsselung ein Standardvorgehen. Es zeigt sich, dass besonders Zahnarztpraxen und Praxen mit sehr gutem IT-Informationsstand am engagiertesten bei der Verschlüsselung von Daten sind.

Für die große Mehrheit der Befragten ist es selbstverständlich, dass es Zugangsbeschränkungen zu den in der Praxis genutzten Geräten gibt. Am meisten wird hier die Passwortsperre eingesetzt, gefolgt von PIN-Sperren. Weitere Beschränkungen sind allerdings eher selten und werden am ehesten von Praxen mit sehr gutem IT-Sicherheitsinformationsstand oder IT-Sicherheitsbeauftragtem eingesetzt.

Maßnahmen zum Schutz der Geräte vor unberechtigten Zugriffen, darunter am häufigsten Bildschirmschoner mit Passwort-Sicherung und die automatische Abmeldung (Timeout), werden von den meisten Praxen umgesetzt. Die größten Defizite bei der Umsetzung von Schutzmaßnahmen gibt es in Praxen ohne IT-Sicherheitsbeauftragten.

Neben dem Standard-Netzwerk verfügt jede dritte Praxis über weitere Netzwerke, beispielsweise Patienten-WLAN oder ein Server-Netz. Am häufigsten trifft das auf größere und geräteintensive Praxen zu.

Der Austausch von Patientendaten mit anderen Leistungserbringern oder Praxen gehört zum Praxisalltag. In der Regel erfolgt dies per Briefpost, Fax oder Telefon oder etwas seltener per E-Mail. Die Auswertungen haben ergeben, dass die klassischen Kommunikationswege in Zahnarztpraxen eine deutlich geringere Rolle spielen. Diese setzen vor allem auf E-Mails und überdurchschnittlich häufig auf Wechseldatenträger und den medizinischen Kommunikationsdienst KIM.

Ein weiterer wichtiger Aspekt der Umfrage im Projekt SiRiPrax war es, Erkenntnisse über IT-Sicherheitsvorfälle in Arztpraxen zu erlangen. Hierbei ging es insbesondere um die Häufigkeit, die Auswirkungen und die Dauer, bis die Praxis wieder einsatzfähig war. Dabei zeigte sich, dass jede zehnte Praxis bereits mindestens einmal von einem IT-Sicherheitsvorfall betroffen war. Bei der Frage nach den häufigsten Auswirkungen wurden Unterbrechungen und Verzögerungen des Praxisalltages, der Ausfall von Systemen und eine erschwerte Wiederherstellung der Daten genannt. In Bezug auf die Wiederherstellung der Daten bestätigten sich die Ergebnisse, dass regelmäßige Sicherheitskopien der wichtigen Daten angelegt und verwaltet werden. Dies unterstreicht auch noch einmal die Sinnhaftigkeit dieser grundlegenden Maßnahme zur IT-Sicherheit.

Die Umfrage in deutschen Arztpraxen hat gezeigt, dass sich die Verantwortlichen in der ambulanten Versorgung mehr Unterstützung bei der Umsetzung einer angemessenen IT-Sicherheit wünschen und diese auch benötigen. Ein Schritt könnte die Überarbeitung der bestehenden IT-Sicherheitsrichtlinie gemäß § 75b SGB V sein. Die Ergebnisse der Umfrage können genutzt werden, um eine Handreichung zu gestalten, die für die Verantwortlichen leichter verständlich und besser umsetzbar ist. Ferner müssen weitere Bestrebungen für die Sensibilisierung unternommen werden, denn die steigende Zahl der Vorfälle weist deutlich darauf hin, dass die IT-Sicherheit auch im Alltag der ambulanten Versorgung immer relevanter wird.

2.3 Medizintechnik

2.3.1 Ausgangslage

Im Rahmen der Digitalisierung stellen immer mehr ursprünglich analoge Geräte „smarte“ Funktionen bereit und bieten eine Vernetzung mit weiteren digitalen Geräten des Alltags, beispielsweise PCs, Smartphones und Clouds. Dieser Trend zeigt sich ebenfalls bei Medizinprodukten. So lassen sich vernetzte Medizinprodukte extern steuern und überwachen. Beispielsweise kann eine Insulinpumpe bequem über das Smartphone gesteuert werden und bietet Nutzenden Funktionen an, die ohne eine App ansonsten nur mittels großen technischen Aufwands im Gerät selbst realisiert werden könnten. Darüber hinaus kann beispielsweise ein Krankenhaus kritische medizinische Geräte auf der Intensivstation über eine Netzwerkschnittstelle zentral überwachen und so deren Funktionsfähigkeit sicherstellen. Des Weiteren ermöglichen bildgebende Geräte wie beispielsweise MRT und CT das Teilen der Messdaten mit Patientinnen und Patienten, weiteren Ärztinnen und Ärzten und der Telematikinfrastruktur. Diese „smarten“ Funktionen bringen allerdings auch Nachteile mit sich: Durch den Einbau von digitalen Schnittstellen und insbesondere durch die Anbindung der Medizinprodukte an weitere Geräte und Netzwerke wird auch die Angriffsfläche vergrößert. Bei analogen Medizinprodukten gab es lediglich die Risiken, dass ein Gerät physisch in seinem Betrieb gestört oder manipuliert werden konnte. Bei vernetzten Geräten besteht jedoch auch die Möglichkeit einer Kompromittierung aus der Ferne. Allerdings tritt solch ein Fall nach den Erfahrungen des BSI nur sehr selten auf. Im Rahmen der Projekte ManiMed[7] und eCare[8] hat das BSI gezeigt, dass die allermeisten vernetzten Medizinprodukte eine hohe Patientensicherheit gewährleisten und die gefundenen IT-Schwachstellen keine ernsthafte Bedrohung darstellen. Doch über das reine Patientenrisiko hinaus kann auch das Risiko bestehen, dass Gesundheitsdaten, die besonders schützenswert sind, durch Angreifende erlangt werden und in fremde Hände geraten.

Das BSI ist der zentrale behördliche Ansprechpartner zur Gewährleistung der Cybersicherheit in vernetzten Medizinprodukten in Deutschland. In Kooperation mit dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) ist das BSI verantwortlich für die Bewertung von Schwachstellen nach § 85 (5) Medizinprodukterecht-Durchführungsgesetz (MPDG) und verfasst Leitfäden und technische Richtlinien zur Prävention von Sicherheitsvorfällen. Beispielsweise gab es Anfang des Jahres 2023 den Verdacht, dass es zu erfolgreichen Angriffen auf eine Insulinpumpe kam, die in wenigen Fällen zu leichten Hyperglykämien aufgrund einer zu geringen abgegebenen Insulindosis führten. Nach einer Prüfung konnte der Verdacht nicht bestätigt werden.

Außerdem führt das BSI Projekte mit Produkttests durch. So ermittelt es den gegenwärtigen Zustand der Cybersicherheit von Produkten auf dem Markt und sensibilisiert Hersteller und Betreiber. Darüber hinaus kooperiert das BSI mit verschiedenen weiteren Behörden und Gremien, insbesondere mit dem Bundesministerium für Gesundheit (BMG). Zudem ist das BSI Mitglied im Expertenkreis CyberMed der Allianz für Cyber-Sicherheit (ACS) sowie vertreten in der Interessengemeinschaft der Benannten Stellen für Medizinprodukte (IG-NB) und verschiedenen Ausschüssen der DIN.

Als nächsten Schritt plant das BSI eine Handlungsempfehlung zu veröffentlichen. Diese basiert auf Ergebnissen bisheriger Projekte und bereits vorhandenen Regularien. Sie ist das Ergebnis des unten im Detail beschriebenen Projekts AnMedPro.

2.3.2 Digitalisierung im Rettungsdienst (eMergent)

eMergent: Warum ist die Digitalisierung des Rettungsdienstes „emergent“?

Die optimale Unterstützung des Rettungsdienstes durch digitalisierte Geräte rettet Leben: Durch Unterstützung in Behandlung, Dokumentation und Einsatzmanagement gewinnen Mitarbeitende im Rettungsdienst Zeit für die medizinische Behandlung.
Die verwendeten Geräte tauschen untereinander Informationen aus und geben einen Überblick über den körperlichen Zustand der Patientinnen und Patienten. Ein früher Informationsaustausch zwischen Leitstelle, Rettungsmittel und Krankenhaus optimiert den Gesamtprozess. Durch moderne Notarztsysteme und die Vernetzung mit Krankenhäusern kann die ärztliche Versorgung bereits frühzeitig beginnen, wo sie in herkömmlichen Szenarien durch Anfahrtswege und fehlendes Personal eingeschränkt war. Darüber hinaus können Fachexperten situationsbedingt hinzugezogen werden. Dabei ist häufig eine gewisse Evolution oder Emergenz zu erkennen: Während zunächst oft klassische analoge Geräte mit neuen Schnittstellen ausgestattet wurden (Vernetzung bestehender Funktionalität), folgte darauf eine Erweiterung durch neue Möglichkeiten digitaler Technik (Vernetzung als Enabler) und letztendlich ein Design neuer Geräte, bei dem die Digitalisierung Teil der Architektur ist (Vernetzung als Designparadigma).

Das Forschungsprojekt eMergent untersuchte die IT-Sicherheit im Kontext der Digitalisierung im Rettungswesen. Im Fokus standen dabei der bodengebundene Rettungsdienst und die dort eingesetzten vernetzten Produkte. Untersucht wurden bereits auf dem Markt verfügbare Geräte, aber auch neue und zukunftsweisende Technologie wurde betrachtet.

eMergent bestand aus drei Teilstudien: einer Orientierungsstudie, einer Anwendendenumfrage und einem Abschlussdokument zu den Sicherheitsuntersuchungen. Die Orientierungsstudie bot Einblicke in den organisatorischen und rechtlichen Rahmen des deutschen Rettungswesens und gab einen Überblick über Produkte, die im bodengebundenen Rettungsdienst eingesetzt wurden. In der Anwendendenumfrage wurde stichprobenartig erfasst, wie Fachkräfte im Rettungsdienst die Digitalisierung und die damit verbundenen Risiken wahrnehmen. Im Rahmen der Sicherheitsuntersuchungen wurden verbreitete Produkte exemplarisch auf Schwachstellen und Risiken untersucht, um durch ein besseres Verständnis der Sicherheitslage potentielle Hilfestellungen und Handlungsbedarf ableiten zu können.

Orientierungsstudie: Status Quo der Digitalisierung im Rettungsdienst

Für den Rettungsdienst ergeben sich spezielle Herausforderungen an die IT-Sicherheit. Aufgrund der mobilen Anwendungsfälle kann physischer Zugriff eines Angreifenden auf die Produkte nicht ausgeschlossen werden. Hinzu kommt, dass der Update-Zyklus für Medizinprodukte durch die Notwendigkeit einer erneuten Zertifizierung oft verlangsamt ist. Eine weitere Besonderheit im Rettungsdienst ist, dass die untersuchten Produkte die Anwendenden entlasten sollen, indem auf automatisierte Sicherheitsmaßnahmen gesetzt wird: Die Rettungsdienstbesatzung hat Expertise in medizinischen Maßnahmen, aber nicht in IT-Sicherheit. Während des Rettungsdiensteinsatzes muss das Personal autonom und zuverlässig arbeiten können.

In der Orientierungsstudie wurden diese Rahmenbedingungen genauer unter die Lupe genommen.
Es wurde analysiert, welche Stakeholder im Rettungsdienst aktiv sind, welche Produkte eingesetzt werden, welche Vernetzungen diese Produkte verwenden und welche regionalen Unterschiede es gibt. Der Betrieb des Rettungsdienstes ist in Deutschland ausgesprochen heterogen und dezentral organisiert. Da der Rettungsdienst in der Hoheit der Bundesländer und oft sogar darunter auf kommunaler Ebene liegt, unterscheidet sich auch die Digitalisierung sehr stark. Entsprechend ist auch die Auswahl und Beschaffung von Geräten für den Rettungsdiensteinsatz von Bundesland zu Bundesland, von Kommune zu Kommune und selbst von Rettungswache zu Rettungswache unterschiedlich umgesetzt. Während es in einigen wenigen Bundesländern einheitliche Vorgaben zum Einsatz von einzelnen Produkten gibt, wird andernorts die Beschaffung dezentral über Ausschreibungen organisiert oder weitgehend der Rettungsdienstorganisation überlassen.

Auch was den allgemeinen Stand der Digitalisierung sowie die Verwendung von digitalen Funktionen und Schnittstellen von Medizinprodukten angeht, ergibt sich kein einheitliches Bild. In einigen Landkreisen gehört es beispielsweise schon zum Tagesgeschäft, Patientendaten, die von einem Monitor aufgenommen werden, automatisch an ein digitales Dokumentationssystem zu übermitteln, das wiederum automatisiert eine Voranmeldung beim Krankenhaus durchführt. In anderen Landkreisen wird dagegen noch mit Stift und Papier dokumentiert.

Für einzelne Geräteklassen ließen sich jedoch auf Basis einer stichprobenartigen Erhebung Trends identifizieren. Es wurde ermittelt, welche Produkte tatsächlich im Einsatz sind und welche in naher Zukunft Verwendung finden könnten. Dabei wurde festgestellt, dass sowohl Medizinprodukte, die einem definiertem Zulassungsverfahren unterliegen, als auch andere Systeme, z. B. für die Einsatzorganisation, das Informationsmanagement und die Dokumentation, eine steigende Relevanz im Rettungsdienst haben. Insgesamt ist der Vernetzungsgrad der einzelnen Systeme erstaunlich hoch und wird tendenziell in der Zukunft noch weiter steigen.

Anwendendenstudie: Wie sieht das Rettungsdienstpersonal die Digitalisierung?

In einer Umfrage durch Selbsteinschätzung, an der 781 Mitarbeitende des Rettungsdienstes teilnahmen, wurde ermittelt, wie Rettungsdienstpersonal die Digitalisierung und die IT-Sicherheit im Rettungsdienst wahrnimmt. Dabei wurde zwischen Entscheidungsträgern wie Führungskräften und Beschaffenden und zwischen Einsatzkräften, im Allgemeinen also der Fahrzeugbesatzung, unterschieden. Entscheidungsträger, die zugleich als Besatzung aktiv waren, erhielten den Fragebogen für Entscheidungsträger. Die Umfrage zielte insbesondere auf die Verwendung und Verbreitung von Geräten, die Erwartungen an die digitalen Eigenschaften dieser Geräte, die Wahrnehmung von IT-Sicherheitsrisiken sowie die Schulung des Personals in Sicherheitsaspekten und den Umgang mit diesen ab. Die Stichprobe war aufgrund der Methodik zur Teilnehmendenakquise sowie auch aufgrund der ungleichen räumlichen Verteilung der Teilnehmenden nicht repräsentativ, lässt aber eine erste Einschätzung zu.

Insgesamt wird Digitalisierung im Rettungsdienst positiv als Arbeitserleichterung aufgenommen. Die Nutzbarkeit steht deutlich gegenüber der IT-Sicherheit im Vordergrund. Bedenken bestanden insbesondere in Bezug auf die Verfügbarkeit bei schlechter Netzabdeckung. Das Risikobewusstsein ist eher stark ausgeprägt, was aber im Kontrast zu einigen Ausprägungen der IT-Sicherheit steht. Die Rückmeldungen zur Vorbereitung und Schulung zeigten Diskrepanzen zwischen Einsatz- und Führungskräften. Etwas weniger als die Hälfte der teilnehmenden Einsatzkräfte fühlte sich ausreichend auf den Umgang mit digitalisierten Geräten vorbereitet, wenige haben eine Einweisung in Datenschutz und IT-Sicherheit erhalten. Eine systematische Betrachtung der IT-Sicherheit scheint oft zu fehlen, beispielsweise ist den Einsatzkräften zu 56 % kein Ansprechpartner für IT-Sicherheitsfragen bekannt und ein Großteil der Führungskräfte gibt an, dass kein ISMS vorhanden ist.

Sicherheitsanalysen: Wie sicher sind Rettungsdienstprodukte tatsächlich?

In den Produkten, die in der Sicherheitsanalyse untersucht wurden, zeigten sich vereinzelt Risiken, beispielsweise durch Standard-Passwörter oder durch gering geschützte Schnittstellen. Im Spannungsfeld zwischen Usability – und damit lebenswichtiger Verfügbarkeit – und IT-Sicherheit nutzen Wachen beispielsweise unsichere Standard-Passwörter, damit auch Aushilfspersonal zuverlässig die Geräte verwenden kann, oder gering geschützte Schnittstellen für eine höhere Interoperabilität mit Krankenhäusern.

Es wurden mehrere Sicherheitslücken systematisch identifiziert und hinsichtlich ihrer Auswirkungen auf die Versorgung von behandelten Personen sowie den Schutz sensibler Daten bewertet. Weiter ergab die Sicherheitsprüfung, dass die Kommunikation zwischen den Geräten größtenteils sicher ist, da auf bewährte Protokolle zurückgegriffen wird. Durch eine aktive Kommunikation zwischen BSI, Sicherheitsexperten und Herstellern konnte die IT-Sicherheit durch eine schnelle Behebung der Schwachstellen gesteigert werden. Im Rahmen des Projektes haben die beteiligten Hersteller angemessen auf die Funde reagiert und diese oft schon während der Analysen behoben.

Die Sicherheit war bei den teilnehmenden Herstellern ein zentrales Thema. Dies zeigte sich in Gesprächen und in ihrer raschen Bereitschaft, identifizierte Schwachstellen zu beheben. Trotz des hohen Stellenwerts der IT-Sicherheit bei den Herstellern und der Bemühungen der Hersteller wurden in fast allen Produkten Schwachstellen festgestellt. Die Schwachstellen wären in der Regel schwer in realistischen Szenarien ausnutzbar. Hierbei ist zu berücksichtigen, dass die Teilnehmenden freiwillig und kooperativ an der Untersuchung teilgenommen haben, sodass die Ergebnisse für die Gesamtheit der Hersteller eventuell nicht repräsentativ sind.

Aus den Erkenntnissen der Studien wurde abgeleitet, welche weiteren Maßnahmen die Hersteller und Betreiber am besten bei einer Verbesserung der IT-Sicherheit unterstützen könnten. Dabei wurde insbesondere Potenzial identifiziert in der Begleitung durch Standards, Best-Practices und bei der Bewertung von Gefahren und Risiken. In vielen Fällen könnte die Sicherheit so bereits mit geringem Aufwand während der Entwicklung der jeweiligen Produkte durch den Hersteller gesteigert werden. Diese Erkenntnisse werden in aktuelle und zukünftige Arbeiten des BSI integriert, beispielsweise in die im Gesundheitswesen einschlägigen Technischen Richtlinien, in folgende Projekte sowie in das Schwachstellenmanagement.

Weitere Informationen

2.3.3 Sicherheit von Wearables mit medizinischen Teilfunktionalitäten (SiWaMed)

In den letzten Jahren werden zunehmend Sensoren in sogenannten Wearables zur Erfassung des Gesundheits- und Fitnesszustands genutzt. Wearables sind kleine Computersysteme, die direkt am Körper getragen werden. So ist es heute möglich, unter anderem die Herzfrequenz, den Blutdruck, den Blutzuckerspiegel, die Sauerstoffsättigung im Blut, das Schlafverhalten oder den Kalorienverbrauch zu messen oder zu berechnen. Wearables verfügen in der Regel über mehrere Schnittstellen und erlauben die Einbindung in Netzwerke. Ebenso sind Wearables häufig mit mobilen Anwendungen (Apps) zur Auswertung und Verwaltung von sensiblen Daten und Erstellung von Statistiken verknüpft.

Obwohl Wearables und deren Komponenten passive Geräte sind, können diese das Verhalten und die Gesundheit der Nutzenden beeinflussen. So könnten mögliche Angriffe auf die Sensorik oder das Übertragungsmedium zu einer Fehleinschätzung des eigenen Gesundheitszustandes führen, die eine potenziell gefährliche Selbstmedikation nach sich ziehen könnte.

Schwachstellen in und an Geräten zur Erfassung von Gesundheits- und Fitnessdaten eröffnen Kriminellen eine neue Form der personenbezogenen Cyberkriminalität. So wäre es zum einen denkbar, dass Wearables gezielt für Angriffe auf Personen verwendet werden, die über eine entsprechende Sensorik verfügen. Auch könnten gezielt Angriffe zur Störung der Genesung von Erkrankten stattfinden, wenn diese beispielsweise ihrer Medikation basierend auf Sensordaten anpassen.

Wer Zugriff auf die von Wearables erfassten Daten hat, kann diese unter Umständen für kriminelle Aktivitäten nutzen, zum Beispiel in Verbindung mit einem Identitätsdiebstahl. Zudem können die Daten für das sogenannte „Doxing“ genutzt werden. Der Begriff wird verwendet, wenn Daten einer Person gezielt beschafft werden, um diese dann im Internet zu veröffentlichen. Oft wird damit das Ziel verfolgt, der Person zu schaden. Zum Beispiel kann durch das Offenlegen „brisanter“ Daten ein Imageverlust von Personen erreicht werden. Ebenso könnten die Opfer eines Datendiebstahls durch Androhung der Offenlegung von Daten erpresst werden.

Daher ist es wichtig, dass Nutzende sich der Risiken der Nutzung bewusst sind.

Im Rahmen des Projektes “Sicherheit von Wearables mit medizinischen Teilfunktionalitäten (SiWamed)” wurde eine Cybersicherheitsbetrachtung für in Deutschland in den Verkehr gebrachte Wearables mit verbauter Sensorik zur Erfassung von Gesundheitsdaten durchgeführt. Zudem wurde ein Überblick über den aktuellen Stand der Technik gegeben. Der Fokus des Projekts lag dabei auf Geräten, die mindestens über Sensorik zur Erfassung der Herzfrequenz und Blutsauerstoffsättigung verfügen, idealerweise ergänzt um eine Sensorik zur Erstellung eines Elektrokardiogramms (EKG).

Im Mittelpunkt der Studie stand die Datensicherheit, d. h. die Gesamtheit der technischen Maßnahmen zum Schutz der verarbeiteten Daten und Wahrung der Integrität, Vertraulichkeit und Verfügbarkeit der Daten. Dazu entwarfen die Testenden maßgeschneiderte Testpläne und analysierten die Wearables mit den zugehörigen Komponenten auf Schwachstellen. Hierbei wurden technisch fortgeschrittene und versierte Angreifer simuliert, denen ein begrenzter Zeitaufwand zur Verfügung stand.

Zur Analyse des Marktes begann das Projekt mit einer Marktstudie, welche die wachsende Bedeutung, Beliebtheit und Nutzung von Wearables belegt. Viele Verbraucherinnen und Verbraucher zögern jedoch bei der Nutzung von Wearables und haben insbesondere Bedenken hinsichtlich der Sicherheit ihrer Daten und Informationen.

Die detaillierte Untersuchung des Wearable-Marktes ergab vier verschiedene, für das Projekt relevante Wearable-Kategorien und Marktsegmente: Smartwatches, Basic Watches, Fitness-Tracker und intelligente Ringe.

Auf der Grundlage der Ergebnisse der Marktumfrage wurden zehn beliebte und aktuelle Wearables als Testobjekte für die technische Sicherheitsbewertung ausgewählt. Die Bewertung beschränkte sich dabei nicht nur auf das Wearable-Endgerät, sondern umfasste auch die damit verbundenen Komponenten Mobile App und Backend-Anwendungen, die typischerweise in Kombination mit dem Endgerät genutzt werden.

Im Rahmen der Sicherheitsanalyse definierten die Testenden eine maßgeschneiderte Reihe von Sicherheitstests für jede Wearable-Komponente. Ziel der ausgewählten Tests war es, einen Überblick über den Schutz und die Sicherheit des Wearable-Endgeräts, der angeschlossenen mobilen App und der Backend-Anwendung zu gewinnen.

Unter den zehn Wearables wurden bei der technischen Bewertung 110 Schwachstellen aufgedeckt, die als „mittel“ oder „hoch“ eingestuft wurden. Keines der Geräte war frei von Schwachstellen.

In Anbetracht der Sensibilität der Daten und Informationen, die von den Wearables mit medizinischen Funktionen verarbeitet werden, werfen die Ergebnisse Fragen und Bedenken auf hinsichtlich der Sicherheit, des verfügbaren Schutzes sowie der Bedeutung, die die Mehrheit der Anbieter und Entwickler dem Schutz der Verbraucherinnen und Verbraucher und ihrer Daten beimisst. Dies ist umso kritischer, wenn man die begrenzte Zeit, die für Tests zur Verfügung stand, sowie die potenziellen Folgen einer Kompromittierung für die Gesundheit der Nutzenden zusätzlich berücksichtigt.

Die Sicherheit und der Schutz von Wearables und ihrer Komponenten muss für Anbieter und Verbraucherinnen und Verbraucher ein wichtiges Anliegen sein.

Durch die Ergebnisse aus dem Projekt sollen Hersteller ermutigt werden, ihre Entwicklungsprozesse und technischen Maßnahmen zum Schutz der Daten zu überprüfen, um die Datensicherheit für die Verbraucherinnen und Verbraucher gewährleisten zu können. Hierzu empfiehlt das BSI die Berücksichtigung von anerkannten Standards in der Industrie und in den Technischen Richtlinien des BSI.

Gleichzeitig sollen die Verbraucherinnen und Verbraucher auf die potenziellen Risiken bei der Nutzung von Wearables aufmerksam gemacht und daran erinnert werden, den Daten und Information der Wearables nicht uneingeschränkt zu vertrauen.

Die Rahmenbedingungen des Projekts haben eine hohe Testabdeckung bei der Prüfung der Wearables nicht zugelassen. Dennoch wurden erhebliche Schwachstellen gefunden – ein Umstand, der dem Schutzbedarf der verarbeiteten Gesundheitsdaten nicht angemessen ist. Angesichts der wachsenden Beliebtheit von Wearables müssen die Datensicherheit und der Datenschutz in den Endgeräten sowie den dazugehörigen mobilen Apps und Backend-Systemen regelmäßig und eingehend überprüft werden.

2.3.4 Digitale Gesundheits- und Pflegeanwendungen

Einen besonderen Platz im Rahmen der Digitalisierung nehmen die Digitalen Gesundheitsanwendungen (DiGA) ein. DiGA sind digitale Anwendungen, die nach § 13 Absatz 1 des Medizinproduktegesetzes als Medizinprodukte in die Risikoklassen I oder IIa eingestuft sind. Im Gegensatz zur Digitalisierung von klassischen Medizinprodukten werden hier nicht Geräte aus dem medizinischen Umfeld miteinander vernetzt, sondern vorhandene digitale Möglichkeiten für eine medizinische Verwendung genutzt. Die Hauptaufgabe einer DiGA besteht darin, bei der Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten, Verletzungen oder Behinderungen zu unterstützen. Versicherte haben einen Anspruch auf die Versorgung

mit diesen Digitalen Gesundheitsanwendungen gemäß § 33a SGB V, sofern die Anwendungen

1. vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) in das Verzeichnis für Digitale Gesundheitsanwendungen nach § 139e SGB V aufgenommen wurden und

2. von Behandelnden, d. h. von Arzt, Ärztin, Psychotherapeut oder Psychotherapeutin, verschrieben oder von der Krankenkasse genehmigt wurden.

Für eine Aufnahme in eben dieses Verzeichnis des BfArM für Digitale Gesundheitsanwendungen muss der Hersteller Nachweise darüber erbringen, dass seine Anwendung

1. den Anforderungen an Sicherheit, Funktionstauglichkeit und Qualität einschließlich der Interoperabilität des Medizinproduktes entspricht,

2. den Anforderungen an den Datenschutz entspricht und die Datensicherheit nach dem Stand der Technik gewährleistet und

3. positive Versorgungseffekte aufweist.

Somit können Patientinnen und Patienten innerhalb ihrer Therapie oder Behandlung eine DiGA verwenden, die beispielsweise bei der Bewältigung von psychischen Erkrankungen unterstützen kann. Derzeit sind 55 Digitale Gesundheitsanwendungen im DiGA-Verzeichnis des BfArM[9] gelistet und können von Leistungserbringern verschrieben werden.

Vergleichbar zu Digitalen Gesundheitsanwendungen beschreibt das SGB XI in § 40a Digitale Pflegeanwendungen (DiPA). DiPA sind Anwendungen für Pflegebedürftige, deren Angehörige oder Pflegepersonal. Diese Anwendungen mindern Beeinträchtigungen der Selbständigkeit oder der Fähigkeiten des Pflegebedürftigen oder wirken einer Verschlimmerung der Pflegebedürftigkeit entgegen. Das schließt auch Anwendungen mit ein, die Pflegende bei der Haushaltsführung unterstützen und die häusliche Versorgungssituation stabilisieren. Anders als bei Digitalen Gesundheitsanwendungen handelt es sich hierbei nicht zwangsläufig um Medizinprodukte.

Das BfArM führt ebenfalls für DiPA ein entsprechendes öffentliches Verzeichnis. Für eine Aufnahme in eben dieses Verzeichnis für Digitale Pflegeanwendungen muss der Hersteller Nachweise darüber erbringen, dass die DiPA

1. die Anforderungen an die Sicherheit, Funktionstauglichkeit und Qualität erfüllt,

2. die Anforderungen an den Datenschutz erfüllt und die Datensicherheit nach dem Stand der Technik gewährleistet und

3. einen pflegerischen Nutzen aufweist.

Um Herstellern und Betreibern mit präventiven Maßnahmen Hilfestellungen geben zu können, wurden Sicherheitsanforderungen für unterschiedliche Teilbereiche von Anwendungen im Gesundheitswesen, worunter auch DiGA und DiPA fallen, verfasst. Die betreffende Technische Richtlinie (TR) umfasst in mehreren Teilen Anforderungen an mobile Anwendungen (TR-03161-1), Web-Anwendungen (TR-03161-2) und Hintergrundsysteme (TR-03161-3)[10].

Die Anforderungen basieren auf dem aktuellen Stand der Technik im Gesundheitswesen, auf den Erkenntnissen aus unterschiedlichen Projekten des BSI sowie auf den gesetzlichen Rahmenbedingungen. Darüber hinaus repräsentieren sie das Ergebnis eines regelmäßigen Austauschs mit der Industrie sowie der Beteiligung des Bundesinstituts für Arzneimittel und Medizinprodukte und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Unter Berücksichtigung der stark fortschreitenden Digitalisierung im Gesundheitswesen sind die gesetzlichen Rahmenbedingungen für DiGA und DiPA

im Wandel. So führt das Digital-Gesetz (DigiG)[11] die Möglichkeit zur Einwilligung in niederschwellige Authentifizierungsverfahren ein. Aufgrund dieses Wandels und des sich weiterentwickelnden Standes der Technik, pflegt das BSI einen regelmäßigen Austausch mit Vertretern der Industrie und den zuständigen Behörden. Die sich hieraus ergebenden Erkenntnisse werden im Rahmen einer jährlichen Evaluierung der TR berücksichtigt und in Form von Anpassungen und Erweiterungen mit aufgenommen.

Für den Nachweis der Konformität gegenüber den beschriebenen Sicherheitsanforderungen bietet das BSI jeweils ein Zertifizierungsverfahren nach TR durch vom BSI anerkannte Prüfstellen[12] an.

2.3.5 Anforderungen an Medizinprodukte (AnMedPro)

Durch unterschiedlichste Digitalisierungsvorhaben ist eine steigende Vernetzung von Medizinprodukten zu beobachten. Dies erfordert es, solche vernetzten Geräte in eine Gesamtinfrastruktur zu integrieren und für verschiedene Einsatzumgebungen einfach und möglichst fehlerfrei einsatzfähig zu gestalten. Um dieses Ziel zu erreichen, müssen sich Medizinproduktehersteller aktiv mit dem Thema Cybersicherheit auseinandersetzen. Potenzielle Bedrohungen durch Cyberangriffe und Manipulationen aus der Ferne können die medizinische Versorgung beeinträchtigen und Patientenleben gefährden.

Medizinprodukte sind oftmals auf einen jahrelangen Einsatz ausgelegt. Zu ihrer Markteinführung können jedoch nur zu dem Zeitpunkt bekannte Cybersicherheitsgefährdungen berücksichtigt werden. Daher müssen auch nach dem Entwicklungsprozess neue Erkenntnisse zu Cybersicherheitsgefährdungen im Lebenszyklus vernetzter Medizinprodukte Berücksichtigung finden, beispielsweise durch zeitnahe Sicherheitsupdates.

Somit rücken bei der Entwicklung von vernetzten Medizinprodukten neben der primären medizinischen Funktion zunehmend auch technische Sicherheitsfunktionen in den Fokus. Nicht nur eine hohe Ausfallsicherheit und Stabilität, sondern auch die Integrität und die Vertraulichkeit der Daten stehen im Mittelpunkt.

Zum einen ist es die Pflicht der Hersteller, der globalen und schnelllebigen Bedrohungslage angemessen entgegenzuwirken und darauf zu reagieren. Zum anderen müssen sie eine Reihe von Gesetzen und regulatorischen Vorgaben berücksichtigen.

Zusätzlich zu den etablierten, teils kritischen medizinischen Funktionen sind aufgrund der Integration und des Ausbaus von Kommunikationsverbindungen technische Maßnahmen zu treffen, die für eine risikoorientierte Absicherung der Produkte sorgen. Die Maßnahmen müssen darauf abzielen, die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen und präventiv zu schützen. Zu dem Spektrum der Maßnahmen zählt unter anderem die Etablierung eines praktikablen Zugriffsschutzes, welcher die besonderen Einsatzumgebungen etwa in Krankenhäusern oder bei den Leistungserbringern ausreichend berücksichtigt. Zudem ist die Absicherung der in den Medizinprodukten vorhandenen Kommunikationsschnittstellen und -verbindungen zu gewährleisten.

Aus diesem Grund werden an Medizinproduktehersteller weltweit diverse Anforderungen in verschiedenen Regelwerken gestellt. Im europäischen Rechtsraum gibt es im Gegensatz zu den USA nur wenige konkrete Vorgaben, wie die IT-Sicherheit von Medizinprodukten zu gestalten ist. Die Grundlagen hierfür sind die europäische Medizinprodukteverordnung (EU) 2017/745 (MDR) sowie die In-vitro-Diagnostika-Verordnung (EU) 2017/746 (IVDR). Diese werden für Hersteller auf dem weltweiten Markt von diversen Regularien anderer Regionen flankiert, z. B. von Regularien der Food and Drug Administration (FDA) aus den USA.

Fokussiert man die Betrachtung auf Aspekte der Cybersicherheit, so wird deutlich, dass die Regularien unterschiedliche Schwerpunkte setzen oder dieselben Schwerpunkte unterschiedlich ausprägen. Diese Heterogenität führt bei den Medizinproduktehersteller zu Unsicherheiten hinsichtlich der Priorität bei der Umsetzung, zumal Maßnahmen zur Erfüllung dieser Anforderungen grundsätzlich durch die Regularien nicht thematisiert werden.

Das BSI kommt seinen gesetzlichen Aufgaben der Erstellung technischer Richtlinien und der Beschreibung und Veröffentlichung sicherheitstechnischer Anforderungen gemäß § 3 Abs. 1 Nr. 6 sowie Nr. 20 BSI-Gesetz (BSIG) nach. Mittels des IT-Grundschutzes des BSI, der einen ganzheitlichen Ansatz zur Informationssicherheit bietet, werden die Anforderungen an sichere vernetzte Medizinprodukte aus den derzeitigen Regularien analysiert und mit praktischen Umsetzungsmaßnahmen konkretisiert.

Zur Ausgestaltung der Umsetzungsmaßnahmen im Rahmen des IT-Grundschutzes wurde die BSI-Arbeitsgruppe AnMedPro (Anforderungen an Medizinprodukte) gegründet. Die Arbeitsgruppe hat das Ziel, eine Guideline für Medizinproduktehersteller zu veröffentlichen, die als Wegweiser bei der Umsetzung der regulatorischen Anforderungen dienen kann. Im Fokus stehen dabei Aspekte der IT-Sicherheit, die die Cybersicherheit für Medizinproduktehersteller umsetzbar machen. Es ist erforderlich, technologieneutral konkrete Maßnahmen aufzuzeigen. In die Entwicklung der Guideline werden Hersteller im Rahmen einer Kommentierung eingebunden, um die Praxisnähe und Praxistauglichkeit nachhaltig gewährleisten zu können.

2.3.6 Sicherheitseigenschaften von Krankenhausinformationssystemen und Austauschformaten (SiKIS)

Mit dem Patientendaten-Schutz-Gesetz (PDSG), das im Oktober 2020 in Kraft getreten ist, gehen erstmals konkrete gesetzliche Vorschriften für die IT-Sicherheit in Krankenhäusern einher. So müssen künftig nicht mehr nur KRITIS-Kliniken ihre Sicherheitsmaßnahmen an einem spezifischen Sicherheitsstandard ausrichten. Laut § 75c SGB V sind seit Januar 2022 alle deutschen Krankenhäuser verpflichtet, „angemessene organisatorische und technische Vorkehrungen“ zu treffen, um die „Verfügbarkeit, Integrität und Vertraulichkeit“ ihrer informationstechnischen Systeme zu gewährleisten. Dabei verweist das Gesetz direkt auf den Branchenspezifischen Sicherheitsstandard (B3S) der deutschen Krankenhausgesellschaft als geeignete Grundlage für die Verbesserung der Informationssicherheit.

Eine erfolgreiche und effiziente Patientenversorgung hängt zunehmend davon ab, wie schnell und sicher alle Beteiligten im Krankenhaus auf die wesentlichen Daten zugreifen können. Hierzu ist es wichtig, dass Daten strukturiert vorliegen. Um einen flüssigen und sicheren Datentransfer zu gewährleisten, müssen Systeme einwandfrei miteinander kommunizieren und interoperabel arbeiten können.

In Krankenhäusern kommen führende Systeme zum Einsatz, um alle Informationen und Daten zu erfassen, zu bearbeiten und zur Verfügung zu stellen. Das Krankenhausinformationssystem (KIS) ist die zentrale Arbeitskomponente, die den medizinischen Versorgungsprozess der Patientinnen und Patienten begleitet. Innerhalb eines KIS werden unter anderem sowohl die administrativen als auch die medizinischen Patientendaten organisiert. Das bedeutet, dass jedes KIS mit einer Vielzahl höchst sensibler Daten agiert und entsprechend gut geschützt werden muss. Denn jede Patientenakte, die in der Regel Befunddaten, Untersuchungsergebnisse, Verordnungen und Therapieentscheidungen beinhaltet, enthält somit schützenswerte personenbezogene Daten. Ferner nehmen KIS eine zentrale Rolle im Behandlungsablauf einer Klinik ein, sodass es beim Ausfall zu Verzögerungen in der Behandlung kommen kann und die Versorgung gefährdet sein könnte.

Häufig handelt es sich bei einem KIS jedoch nicht um ein monolithisches System, sondern vielmehr um eine Sammlung von Komponenten, die von einem oder mehreren Herstellern stammen und unterschiedliche Spezialisierungen aufweisen. Neben dem KIS gibt es noch weitere ähnlich arbeitende Informationssysteme, beispielsweise Laborinformationssysteme (LIS) oder Radiologieinformationssysteme (RIS). Die große Menge an verfügbaren Daten und die damit einhergehenden hohen Anforderungen an die IT-Sicherheit und den Datenschutz machen jedes KIS zu einem enorm komplexen Gebilde. Damit all diese Systeme interoperabel zusammenarbeiten können und ein Datentransfer möglich ist, werden Schnittstellen mit standardisierten Datenformaten benötigt. Die technischen Voraussetzungen hierfür sind durch offene, internationale Standards und Profile (z. B. HL7, FHIR, DICOM und IHE) zum Datenaustausch speziell für das Gesundheitswesen durchaus gegeben. Im deutschen Gesundheitswesen zeigt sich jedoch, dass diese internationalen Standards und Profile als Grundlage der Interoperabilität nicht effektiv angewendet werden können, weil es zahlreiche unterschiedlich ausgeprägte Entwicklungen von proprietären Systemen sowie individuell realisierte technische Standards gibt.

Diese Problematik hat der Gesetzgeber erkannt und in den letzten Jahren einige gesetzgebende Maßnahmen hervorgebracht. Mit dem Ausbau der Telematikinfrastruktur (TI) sowie dem Krankenhauszukunftsgesetz (KHZG) wurden Schritte zur weiteren Digitalisierung und Interoperabilität von Daten in Deutschland eingeleitet. So wurden beispielsweise mit § 373 Abs. 5 SGB V die Vorgaben für Krankenhäuser eingeführt, dass nur noch von der gematik bestätigte „Informationstechnische Systeme im Krankenhaus (ISiK)“ eingesetzt werden dürfen, welche grundlegende Interoperabilitätsanforderungen erfüllen. Der ISiK-Standard basiert auf dem HL7-FHIR-Standard. Im ISiK-Standard werden die Anforderungen, die von den betroffenen Einrichtungen einzuhalten sind, in Form von unterschiedlichen Modulen nacheinander eingeführt. Die Umsetzung des ISiK-Standards bringt auf lange Sicht diverse Vorteile. So kann Zeit gespart werden, da Daten automatisch zwischen Systemen, auch zwischen Systemen unterschiedlicher Einrichtungen, z. B. Krankenhäusern und Reha-Kliniken, ausgetauscht werden können. Gleichzeitig wird die Anfälligkeit für Übertragungsfehler gesenkt.

Durch die Nutzung neuer interoperabler Standards wird eine Vernetzung von Systemen weiter gefördert, wodurch auch neue bestimmte Risiken entstehen. Wenn Schwachstellen zu Systemausfällen führen oder Angreifende ein System über eine Schwachstelle kompromittieren, ermöglichen angebundene Systeme eine zusätzliche Ausweitung und beeinträchtigen somit andere Bereiche der Versorgung. So können ganze Systemlandschaften betroffen sein. Dies hat Auswirkungen auf den Betrieb des Krankenhauses und damit auf die Versorgung. Da diese Systeme in vielen Krankenhäusern und Versorgungszentren eine zentrale Rolle spielen und als Schnittstelle zwischen unterschiedlichen anderen Anwendungen fungieren, muss hier der Aspekt der IT-Sicherheit besonders berücksichtigt werden.

Daher plant das BSI im Rahmen der Studie SiKIS (Sicherheitseigenschaften von Krankenhaus-Informationssystemen) sowohl die verwendeten Standards als auch die in Deutschland eingesetzten KIS näher zu betrachten. Der Fokus dieser Studie liegt auf der IT-Sicherheit. Konkret soll untersucht werden, ob es Möglichkeiten gibt, diese branchenspezifischen Standards sicher zu implementieren, und welche Funktionen von derzeit auf dem Markt existierenden KIS realisiert werden müssen, um einen sicheren Betrieb zu gewährleisten. Aus diesem Grund gliedert sich das Projekt in mehrere Teile. Zunächst sollen in einem theoretischen Teil die grundlegenden Probleme beim Einsatz der branchenspezifischen Austauschformate diskutiert werden. Darüber hinaus werden die in Deutschland eingesetzten KIS und deren Funktionen sowie Schnittstellen näher betrachtet. Dies soll dabei helfen, abzuschätzen, ob in einem zweiten Teil anhand von praktischen Tests in dedizierten Laborumgebungen neue Erkenntnisse zu vorhandenen Schwachstellen oder Fehlern bei der Implementierung gewonnen werden können. Ziel des gesamten Projektes ist es, dann im Abschluss diese Erkenntnisse als praktische Empfehlungen zu veröffentlichen, um die IT-Sicherheit in der Krankenhauslandschaft zu erhöhen.

3. Ausblick

Das Jahr 2023 hat gezeigt, dass die Cybersicherheitslage auch im Gesundheitswesen weiterhin angespannt ist. Insgesamt war in allen Digitalisierungsbereichen Deutschlands eine deutliche Zunahme an aufgedeckten Software-Schwachstellen zu verzeichnen. So stellt es der Bericht zur Lage der IT-Sicherheit in Deutschland unter www.bsi.bund.de/lagebericht dar.

Häufig lässt sich solchen Schwachstellen mit relativ einfachen Maßnahmen entgegentreten. Diese Maßnahmen müssen von den Nutzerinnen und Nutzern allerdings auch akzeptiert und angewendet werden.

Gleichzeitig muss gerade im Gesundheitswesen beim Einführen von Sicherheitsmaßnahmen, wie beispielsweise einer aufwändigen Zugriffskontrolle für Medizinprodukte, gewährleistet sein, dass Informationen im Ernstfall verfügbar sind und damit die Patientensicherheit erhalten bleibt.

Der Schwerpunkt der Arbeiten des BSI im Jahr 2024 wird aus diesem Grund darauf liegen, Cybersicherheit bis hin zur Code-Ebene so pragmatisch wie möglich zu gestalten – durch klare, umsetzbare Empfehlungen und Vorgaben sowie eine konkrete, realistische Vorstellung davon, wie die IT-Produkte und Anwendungen des Gesundheitswesens von morgen aussehen müssen.

Literatur-verzeichnis

[01] https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/gesundheitsdatennutzungsgesetz.html

[02] https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/digig

[03] https://fachportal.gematik.de/fileadmin/Fachportal/Downloadcenter/gemKPT_Zero_Trust_V1.0.0.pdf

[04] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Zero-Trust/zero-trust.html

[05] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Beschleunigte-Sicherheitszertifizierung/beschleunigte-sicherheitszertifizierung_node.html

[06] https://www.gematik.de/newsroom/news-detail/pressemitteilung-spezifikation-ti-gateway-veroeffentlicht

[07] Abschlussbericht ManiMed: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/ManiMed_Abschlussbericht.html

[08] Abschlussbericht eCare: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/eCare_Abschlussbericht.html

[09] https://diga.bfarm.de/ (Stand: November 2023)

[10] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03161/tr-03161.html

[10] https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/digital-gesetz.html

[12] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Liste-TR-Pruefstellen/liste-tr-pruefstellen.html

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
53175 Bonn
Tel.: 0 800 274 1000

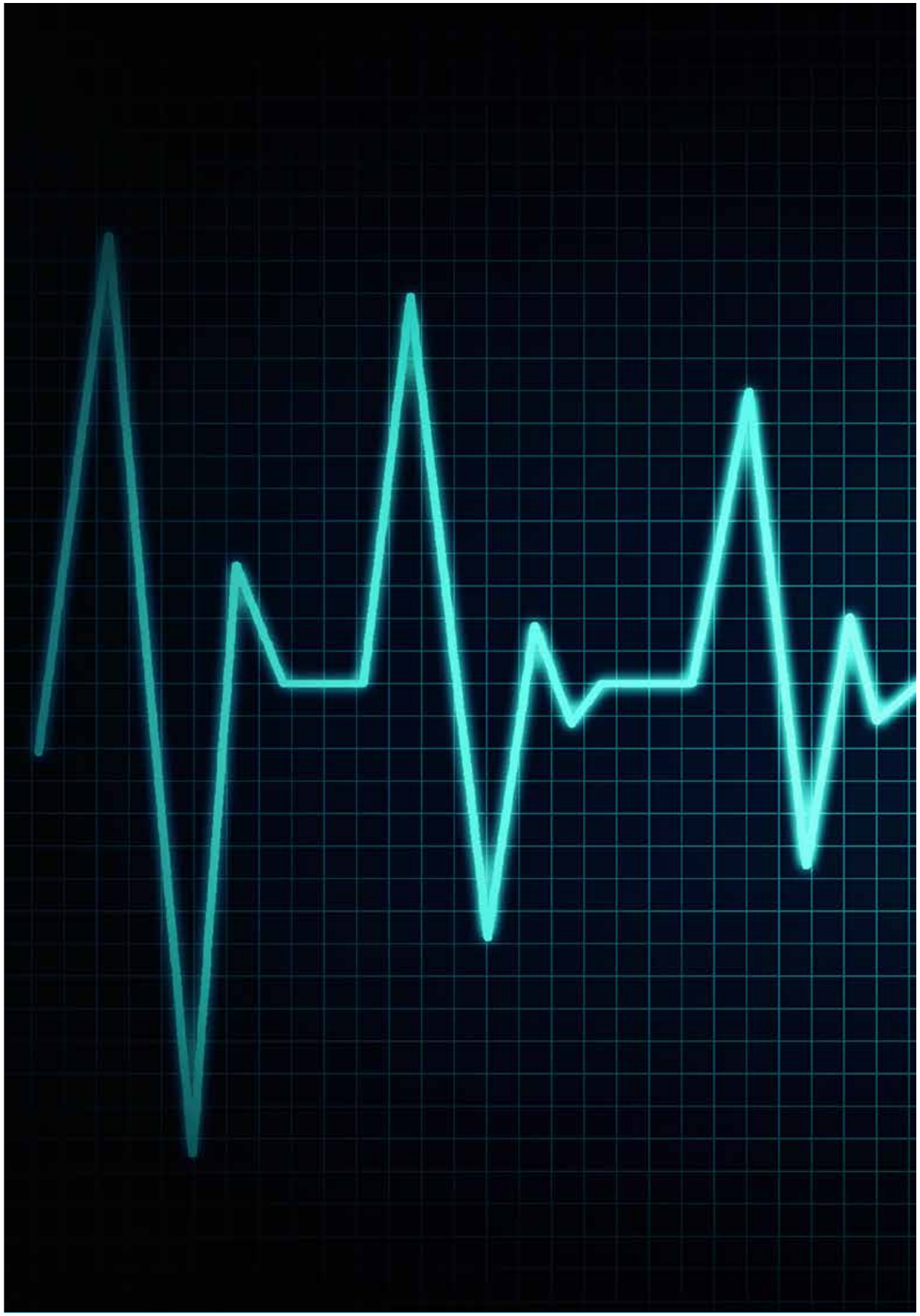
Kontakt
referat-di24@bsi.bund.de

Stand
April 2024

Konzept und Gestaltung
Bundesamt für Sicherheit in der Informationstechnik

Druck
Appel und Klinger Druck & Medien GmbH
Bahnhofstraße 3
96277 Schneckenlohe
www.ak-druck-medien.de

Bildnachweis
Titel: AdobeStock © bittedankeschön; Seite 2: AdobeStock © Zsolt Biczó; Seite 4/5: AdobeStock © ipopba; Seite 6/7: AdobeStock © MQ-Illustrations; Seite 8: AdobeStock © titima157; Seite 11: AdobeStock © TenWit; Seite 13: AdobeStock © sodawhiskey; Seite 15: AdobeStock © Gorodenkoff; Seite 16: AdobeStock © shevchukandrey; Seite 18: AdobeStock © peterschreiber.media; Seite 20: AdobeStock © VanHope; Seite 23: © MHD Koblenz e. V. (eigenes Bild); Seite 22: © MHD Koblenz e. V. (eigenes Bild); Seite 25: AdobeStock © sitthiphong; Seite 26: AdobeStock (c)Anna Stills; Seite 29: AdobeStock © Vadim; Seite 30: AdobeStock © Kzenon; Seite 32: AdobeStock © Elnur; Seite 35: AdobeStock © Zsolt Biczó



Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
E-Mail: bsi@bsi.bund.de
www.bsi.bund.de