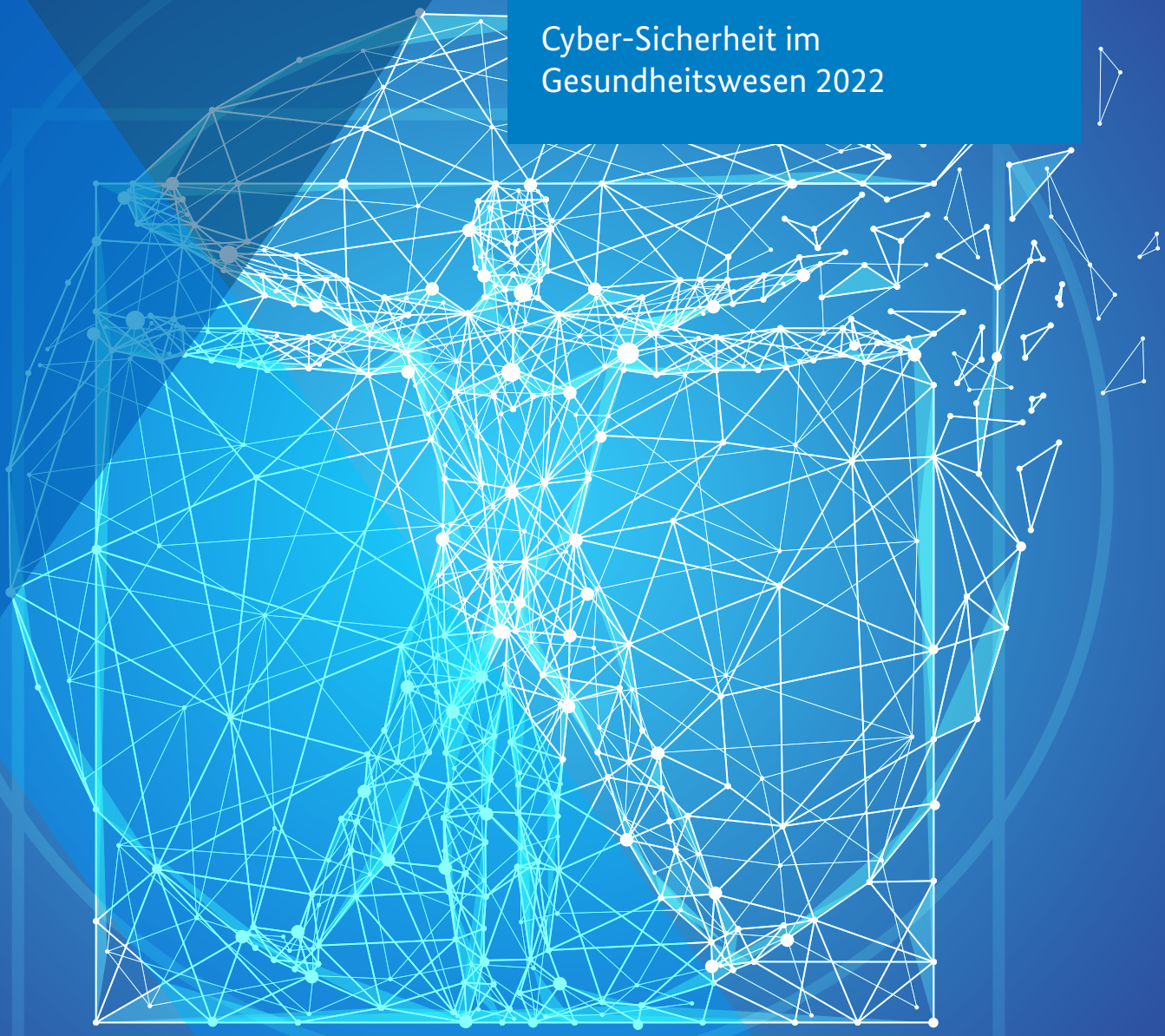
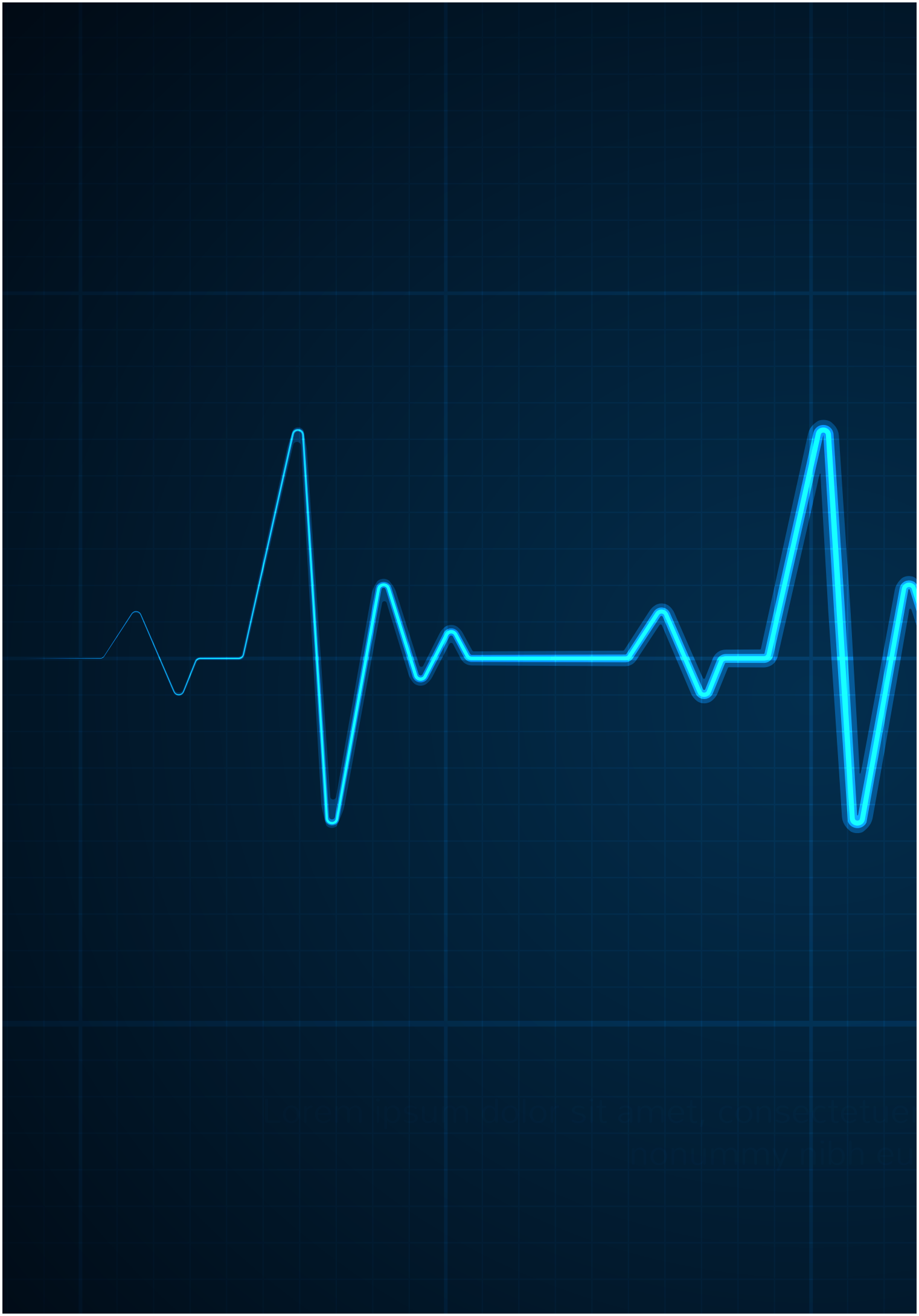
Lagebild Gesundheit

Cyber-Sicherheit im Gesundheitswesen 2022



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•



Inhalt

1. Einleitung

Das BSI gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft, als Voraussetzung einer erfolgreichen Digitalisierung. Die ganzheitliche Umsetzung dieser Aufgabe im Bereich des Gesundheitswesens ist dabei eine komplexe und vielfältige Herausforderung, sowohl für die Industrie als auch die zuständigen Behörden.

Das vorliegende „Lagebild Gesundheit“ soll zum ersten Mal die Sicherheitslage im Gesundheitswesen aus Sicht des Bundesamtes für Sicherheit in der Informationstechnik darstellen. Betrachtet werden die Bereiche der Telematikinfrastruktur, der digitalen Gesundheitsanwendungen, der Medizinprodukte, der digitalen Pandemiebekämpfung sowie der Sicherheitslage in der ambulanten Versorgung. Dabei führt Kapitel 2 allgemein in die jeweilige Digitalisierungsaktivität ein und Kapitel 3 beleuchtet die Cyber-Sicherheit innerhalb des jeweiligen Themas.

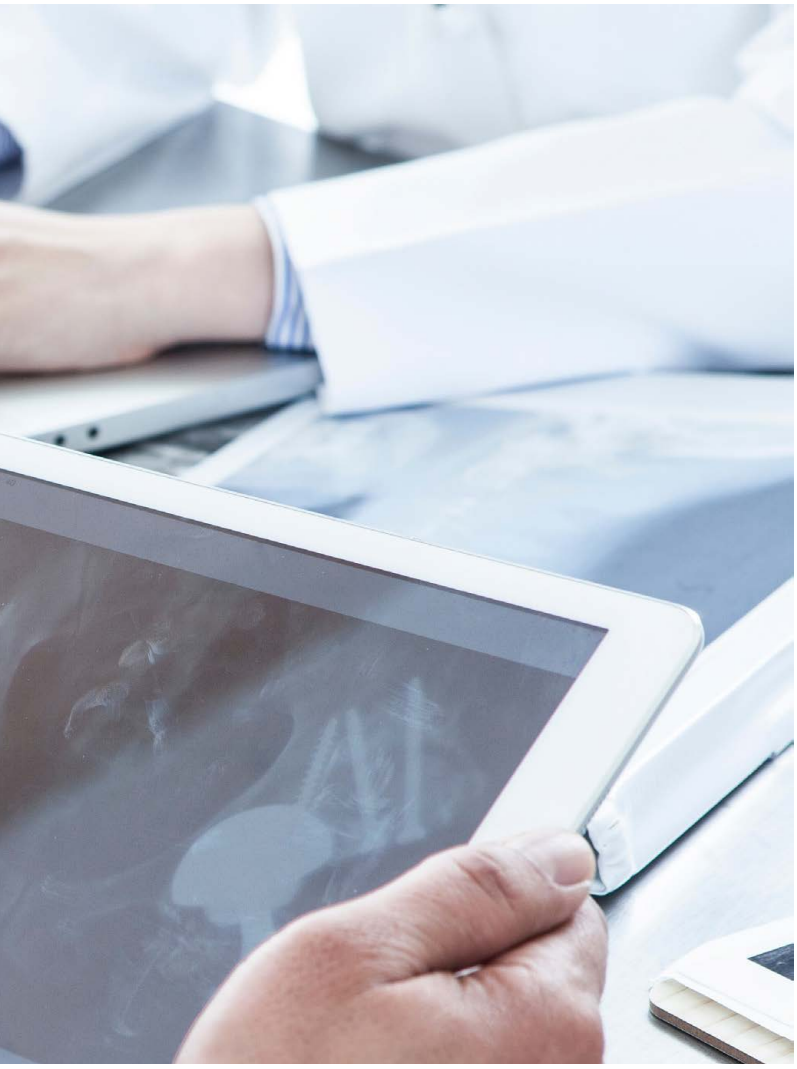
2. Digitalisierungs-bereiche des Gesundheitswesens

2.1 Telematikinfrastruktur

Die Telematikinfrastruktur (TI) blickt bereits auf einen langen Entwicklungsprozess zurück und muss sich fortwährend an den technischen Wandel und die sich hieraus ergebenden neuen technischen Chancen und Gefährdungen anpassen. Sie hat ihre Ursprünge im Jahr 2002, als Reaktion auf den Lipobay-Skandal. Durch die Einführung einer elektronischen Gesundheitskarte sollten schädliche Wechselwirkungen vermieden werden – was heute noch als elektronischer Medikamentenplan (eMP) und Arzneimitteltherapiesicherheit (AMTS) wichtige Anwendungen der TI darstellt. 2011 wurde die erste Generation der elektronischen Gesundheitskarte (eGK G1) eingeführt, damals noch ohne nennenswerte zusätzliche Funktionen. Erst 2015 wurden mit dem E-Health-Gesetz die gesetzlichen Grundlagen für die heutigen Funktionen der Telematikinfrastruktur geschaffen, darunter die elektronische Patientenakte (ePA), Notfalldatenmanagement (NFDM), Videosprechstunde und viele weitere Anwendungen.

Heute steht der Telematikinfrastruktur ein weiterer Wandel bevor. Die klassische, auf sicheren Komponenten zum Netzzugang (Konnektoren) basierende, Architektur soll an die Lebensrealität der Versicherten angepasst werden. Hierbei sollen statt überwiegend stationären Anwendungsfällen beim Leistungserbringer, auch die fortschreitende Digitalisierung durch mobile Endgeräte der Versicherten einbezogen werden. Hierdurch können ebenfalls neue Anwendungsfelder der mobilen Versorgung erschlossen werden.

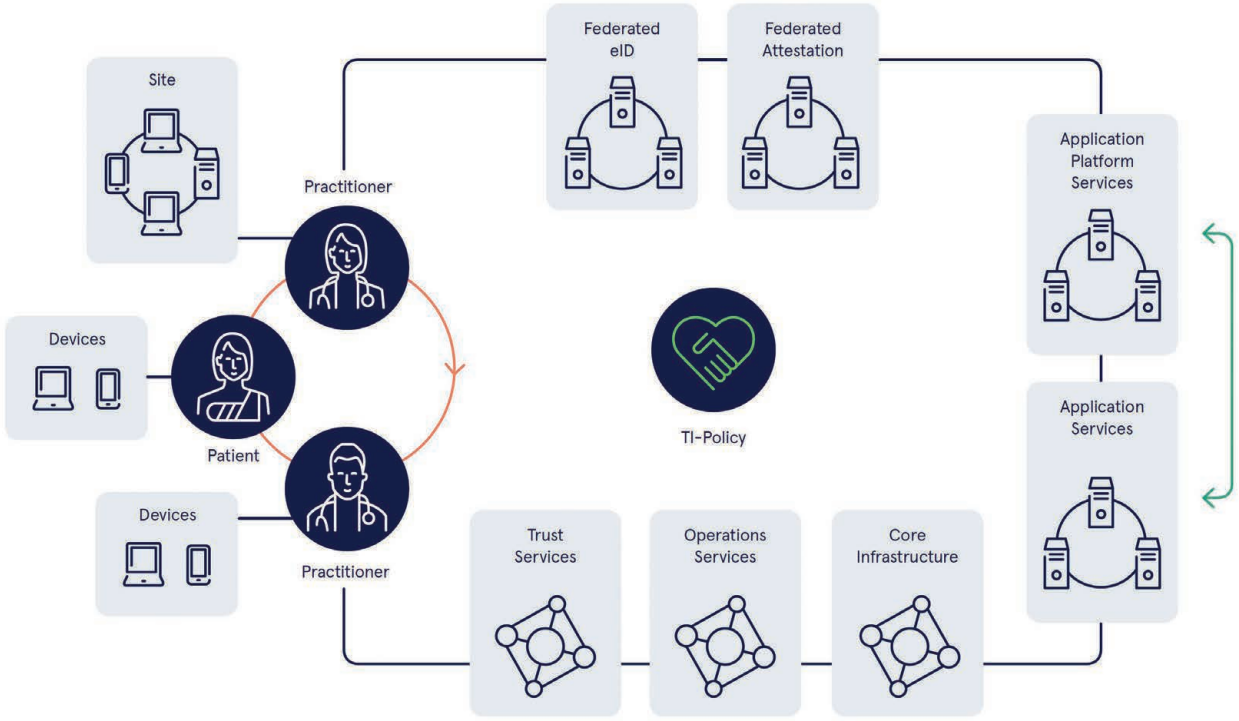
Abschnitt 2.1 bietet einen Überblick über den Wandel zu TI 2.0. Nähere Informationen zu Anwendungen in Arzt- und Zahnarztpraxen folgen in Abschnitt 2.4 (elektronischen Patientenakte (ePA), Kommunikation im Medizinwesen (KIM), elektronische Arbeitsunfähigkeitsbescheinigung (eAU) und E-Rezept).



2.1.1 Ein Gesundheitssystem im Wandel

Die Telematikinfrastruktur (TI) der gematik GmbH bildet die staatlich geförderte Vernetzung des Gesundheitswesens und damit die grundlegende Infrastruktur eines digitalisierten Gesundheitswesens in Deutschland. In den vergangenen 20 Jahren durchlebte sie einen Wandel durch neue Rahmenbedingungen, Anforderungen der Bedarfsträger und technologische Möglichkeiten. Neue Anwendergruppen und Anwendungsfälle machen ein Überdenken erforderlich, was sich als eine Neuarchitektur – die Telematikinfrastruktur 2.0 (TI 2.0) – niederschlägt. Das Bundesamt für Sicherheit in der Informationstechnik begleitet dieses Vorhaben gemäß der gesetzlichen Zuständigkeit.

Abbildung 1: Planung der gematik GmbH zur TI 2.0-Architektur



Quelle: gematik GmbH, 2020, Arena für digitale Medizin – Whitepaper TI 2.0

2.1.2 Was ist die TI 2.0?

Die Erwartungen an die Digitalisierung des Gesundheitswesens haben sich derart verändert, dass sich die gematik GmbH für eine Neuarchitektur der TI entschied. Hierdurch wachsen verschiedene Versorgungsbereiche zusammen. Die initialen Anwendungsfälle der Ärztinnen und Ärzte sowie Versicherten wurden bereits um die Perspektive der Apothekerinnen und Apotheker, sowie die der Krankenkassen erweitert. Nun werden weitere Leistungserbringer eingebunden wie Physiotherapierende, Hebammen, Pflegedienste und private Krankenversicherungen. Zudem werden die Anwendungen der Telematikinfrastruktur mit Gesundheitsanwendungen anderer Bereiche verknüpft, wie Digitale Gesundheits- und Pflegeanwendungen (siehe Kapitel 2.2.2), Implantate und ein europaweiter Austausch von Notfalldaten.

Natürlich erfordern tiefe Eingriffe in eine Architektur konzeptionelle Planungen. Diese stecken derzeit noch in den Anfängen und stellen im ambitionierten Zeitplan eine Herausforderung dar. Das BSI unterstützt als zuverlässiger Partner die Planungen durch Beratung. Hierbei gewährleistet das BSI entsprechend seiner gesetzlichen Vorgaben aber auch als „Geist, der stets verneint", ebenfalls bei Zeit- und Kostendruck die Qualität der IT-Sicherheit. Die gematik GmbH besitzt wirksame Sicherheitsmechanismen auf den Ebenen der Sicherheitskonzeption, der Begleitung und Zulassung von Herstellern und ihren Diensten und Komponenten, sowie in der Überwachung des Betriebes. Das BSI ergänzt dies um seine Expertise als unabhängige Zertifizierungsstelle und durch die Begutachtung der Sicherheitskonzeptionen. Diese Kooperation ist notwendig, da bei einer gebündelten Verantwortung für Planung, Umsetzung und Zulassung bei der gleichen Stelle Interessenkonflikte unvermeidlich wären.

2.1.2.1 Welche Mindestanforderungen stellt das BSI?

Um im frühen Planungsstand bereits in die Diskussion einzusteigen, einigten sich das BSI und die gematik GmbH auf folgende zehn grundlegende Sicherheitssäulen:

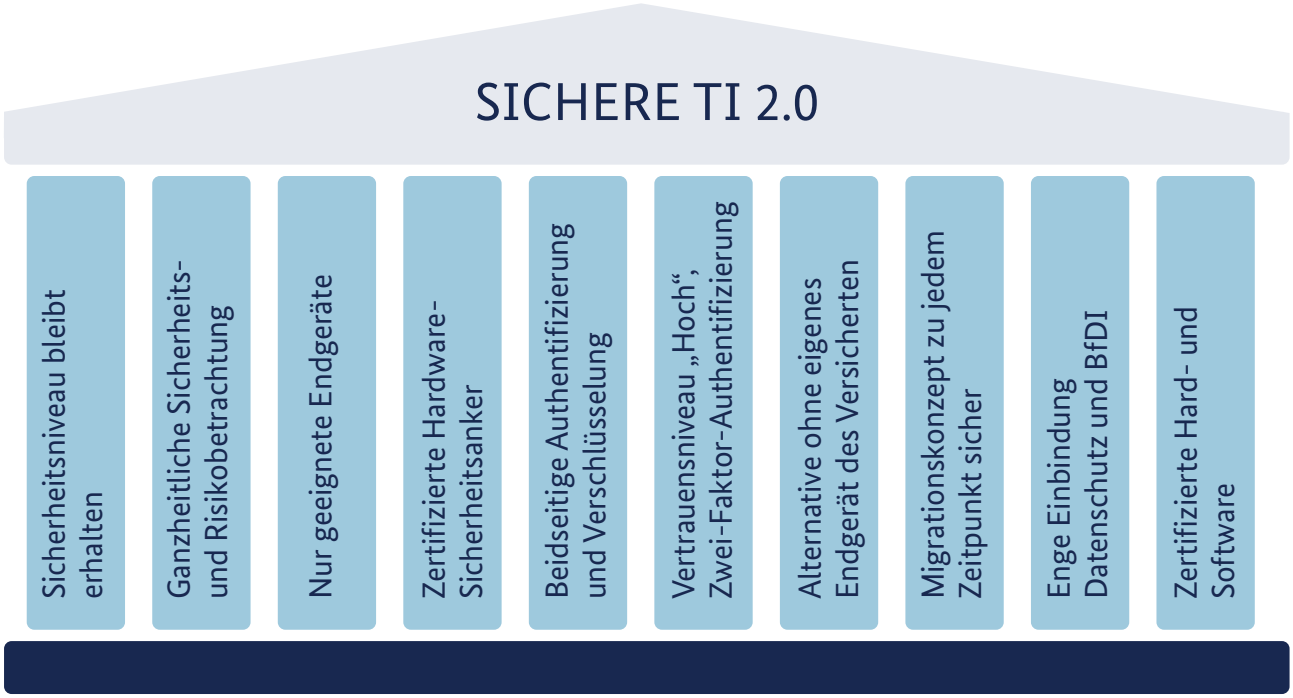
1. Das bisherige Sicherheitsniveau muss auch unter der neuen Architektur gemäß den Schutzbedarfs-Definitionen und -Feststellungen gewährleistet sein.
   Dies lässt selbstverständlich den Spielraum, Sicherheitsvorkehrungen an die aktuellen Rahmenbedingungen der Einsatzumwelt anzupassen und den aktuellen Stand der Technik zu berücksichtigen. Die Säule soll Veränderungen nicht durch veränderungsfreie Sicherheitsanforderungen verhindern, sondern das erforderliche Vertrauen in den Schutz besonders sensibler medizinischer Daten fortsetzen.
2. Zur Wahrung eines durchgängigen und angemessenen Schutzniveaus müssen die bestehenden Sicherheits- und Risikoanalysen aktualisiert und

ggf. erweitert werden. Die Analysen sollten durch eine ganzheitliche Betrachtung der Prozesse und Systeme erfolgen.
Dies bedeutet auch, dass Risiken, die für den Anwender durch Veränderungen in der Konzeption ausgehen auf Ebene der Risikobetrachtung mit einbezogen werden müssen.

3. Die für die Verarbeitung vertraulicher medizinischer Daten verwendeten Endgeräte müssen über ein geeignetes Sicherheitsniveau verfügen. Dies muss technisch unterstützt werden.
4. Die kryptographische Sicherheit muss auf einem zertifizierten Hardware-Sicherheitsanker basieren. Dieser muss unter alleiniger Kontrolle des Data-Owners sein. Nur unter dieser Voraussetzung ist eine Auslagerung nachfolgender kryptographischer Prozesse grundsätzlich möglich.
5. Jegliche Kommunikationsverbindung muss beidseitig authentifiziert und verschlüsselt sein.
6. Anwender müssen durch eine Zwei-Faktor-Authentifizierung authentifiziert werden, wobei beide Faktoren das Vertrauensniveau „hoch“ erreichen.
7. Für alle Dienste der Versicherten muss es eine im Alltag zumutbare und leicht verfügbare Alternative geben, falls die versicherte Person nicht über entsprechende Endgeräte verfügt oder die Sicherheit des Endgerätes nicht sichergestellt werden kann, respektive das Risiko dafür nicht tragen will.
8. Die Migration wird einen zeitweisen Parallelbetrieb erfordern. Neben der Ausgestaltung der TI 2.0 ist daher auch ein detailliertes Migrationskonzept essentiell, um die Risiken bei der Migration komplexer Systeme zu minimieren.
9. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wird eng eingebunden.
10. Wo erforderlich, kommen weiterhin entsprechend der gesetzlichen Vorgaben zertifizierte Komponenten und Dienste zum Einsatz.

Hiermit sind die Grundpfeiler der neuen Architektur bereits frühzeitig zwischen der gematik GmbH und dem BSI vereinbart worden. Dies bietet das Fundament der neuen und noch zu konzipierenden Architektur der TI 2.0.

Abbildung 2: Sicherheitssäulen der TI 2.0



Quelle: BSI

2.2 Medizinprodukte

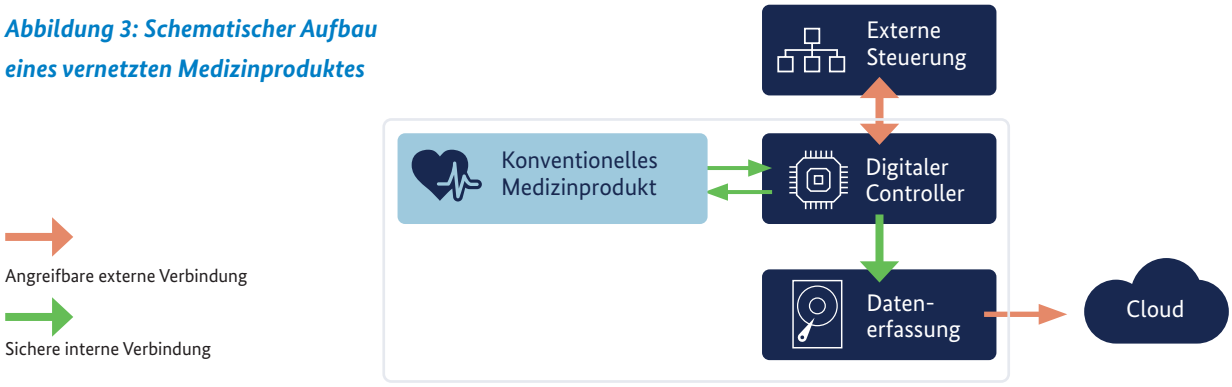
In vielen Bereichen im Gesundheitswesen unterstützen und erleichtern Medizinprodukte die Arbeit und den Alltag von Ärztinnen und Ärzten, Pflegekräften und Patientinnen und Patienten. Insbesondere auf Intensivstationen und im Rettungsdienst sind sie essentiell, um Vitalfunktionen zu überwachen und existentiell lebensnotwendige Funktionen, insbesondere die Beatmung, autonom sicherzustellen. Außerdem helfen sie in der Diagnostik, indem sie beispielsweise bildgebende Verfahren, z.B. Computertomographie (CT) und Magnetresonanztomographie (MRT), bereitstellen. In zunehmendem Umfang unterstützen mobile Medizinprodukte auch bei der Behandlung zu Hause und im normalen Alltag, beispielsweise in Form von Herzschrittmachern und Insulinpumpen. Medizinprodukte werden kontinuierlich weiterentwickelt und erhalten im Rahmen der Digitalisierung immer mehr „smarte“ Funktionen und erschließen hiermit mitunter auch neue Bereiche.

2.2.1 Vernetzung von Medizinprodukten

Sogenannte „smarte“ Medizinprodukte bieten zunehmend eine Vernetzung mit weiteren digitalen Geräten des Alltags – beispielsweise PCs, Smartphones und sogar Clouds. Dieser Trend zeigt sich ebenfalls bei Medizinprodukten. So lassen sich vernetzte Medizinprodukte extern steuern und überwachen. Beispielsweise kann eine Insulinpumpe komfortabel und visuell über das Smartphone gesteuert werden und bietet den Nutzerinnen und Nutzern Funktionen an, die ohne eine App nur mittels großem technischen Aufwand im Gerät 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 beispielsweise das Speichern in einer elektronischen Patientenakte.

Alle diese Funktionen werden durch digitale Controller und Schnittstellen ermöglicht, die in das konventionelle Medizinprodukt integriert werden. In Abbildung 3 ist der Aufbau eines vernetzten Medizinproduktes schematisch dargestellt. Die Erweiterung des digitalen Controllers erlaubt eine externe Anbindung und stellt eine Datenerfassung bereit. Dadurch können die Produkte im Vergleich zu ihren Vorgängern komplexe, sensorgesteuerte und vom Nutzer konfigurierbare „smarte“ Funktionen ausführen. Zudem erlauben diese eine Protokollierung von gemessenen Sensordaten und eine externe Steuerung über Schnittstellen, worüber Benachrichtigungen und Warnungen ausgegeben werden können. Dieser Fortschritt erlaubt eine einfachere und gezieltere Behandlung im Vergleich zu konventionellen Produkten.

Abbildung 3: Schematischer Aufbau eines vernetzten Medizinproduktes



Quelle: BSI

2.2.2 Digitale Gesundheits- und Pflegeanwendungen

Vor dem Hintergrund der Einschätzung des Bundesministeriums für Gesundheit stehen die Gesundheitssysteme der westlichen Welt vor großen Herausforderungen. Es gilt immer mehr ältere und chronisch erkrankte Menschen zu behandeln, teure medizinische Innovationen zu bezahlen und strukturschwache ländliche Gebiete medizinisch zu versorgen [1]. Hierbei bieten digitale Anwendungen im Gesundheitswesen das Potential solche und andere Herausforderungen besser zu lösen. Sie haben das allgemeine Ziel bei „der Behandlung und Betreuung von Patientinnen und Patienten“ zu unterstützen und „die Möglichkeiten [zu] nutzen, die moderne Informations- und Kommunikationstechnologien (IKT) bieten“ [2].

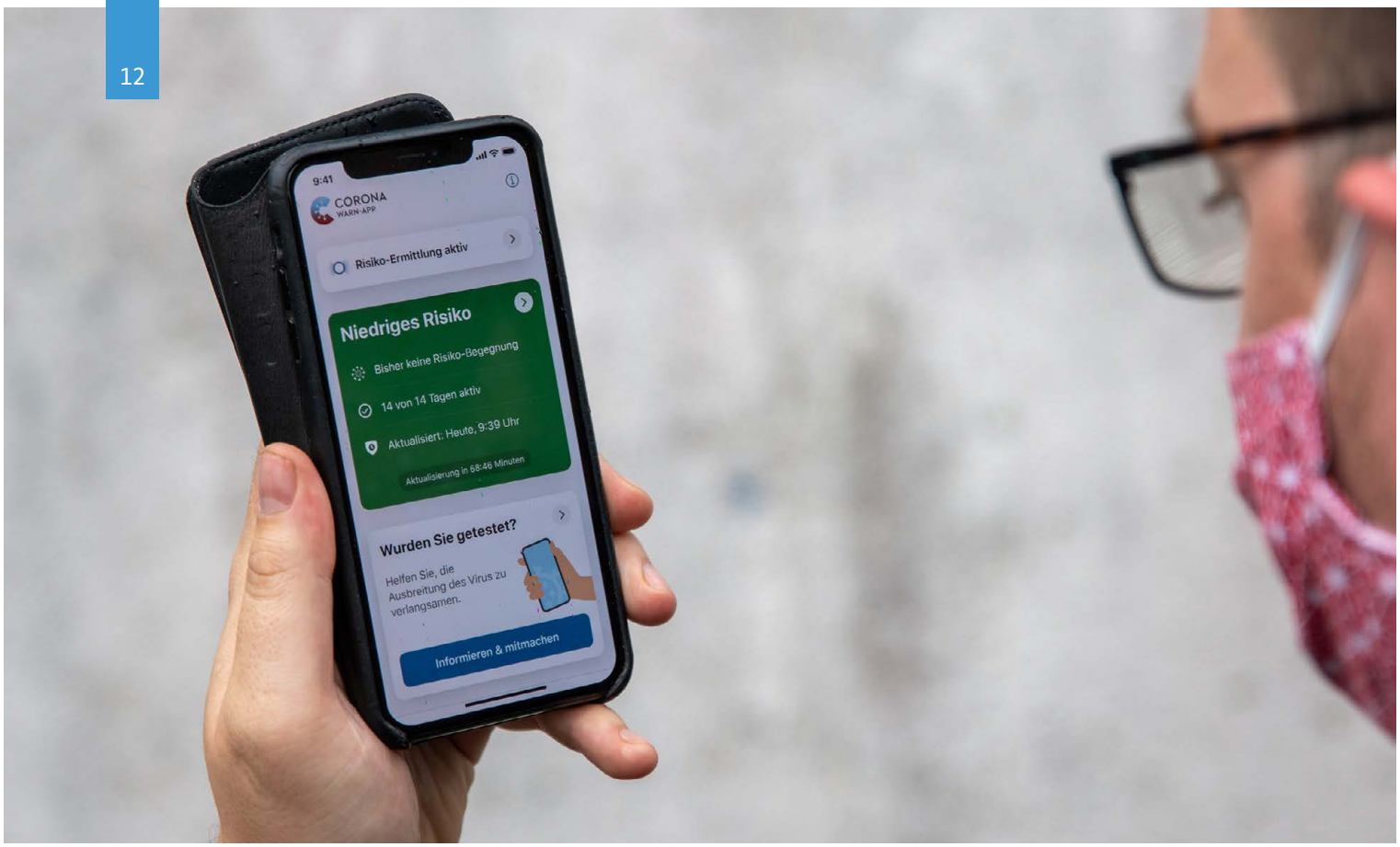
Einen besonderen Platz nehmen hierbei die digitalen Gesundheitsanwendungen (DiGA) ein. DiGAs sind als Medizinprodukte der Risikoklasse I oder IIa nach § 13 Absatz 1 des Medizinproduktegesetzes eingestufte digitale Anwendungen. Im Gegensatz zu klassischen Medizinprodukten besteht die Digitalisierung nicht aus der Vernetzung eben dieser Medizinprodukte, sondern aus der medizinischen Verwendung digitaler Möglichkeiten. 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 sie

1. vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) in das Verzeichnis für digitale Gesundheitsanwendungen nach § 139e SGB V aufgenommen wurden und
2. von der behandelnden Ärztin oder dem behandelnden Arzt, der Psychotherapeutin oder dem Psychotherapeuten 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 bzw. Behandlung eine DiGA verwenden, welche bspw. bei der Bewältigung von psychischen Erkrankungen unterstützen kann. Derzeit sind 43 digitale Gesundheitsanwendungen im DiGA-Verzeichnis des BfArM gelistet [3] und können von Leistungserbringern verschrieben werden (Stand: 22. Dezember 2022).



Vergleichbar zu digitalen Gesundheitsanwendungen beschreibt das SGB XI in § 40a digitale Pflegeanwendungen (DiPA). DiPAs sind Anwendungen für Pflegebedürftige, für deren Angehörige oder das Pflegepersonal, welche Beeinträchtigungen der Selbständigkeit oder der Fähigkeiten des Pflegebedürftigen mindern oder einer Verschlimmerung der Pflegebedürftigkeit entgegenwirken. Das schließt auch Anwendungen mit ein, die Pflegende bei der Haushaltsführung unterstützen und die häusliche Versorgungssituation stabilisieren. Anders als bei digitalen Gesundheitsanwendungen handelt es ich hierbei jedoch nicht notwendigerweise um Medizinprodukte. Das BfArM führt ebenfalls für DiPAs 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 einen Nachweis der Datensicherheit für DiGA und DiPA zu ermöglichen, hat das BSI in einer Reihe von Technischen Richtlinien unter der Nummer 03161 „Anforderungen an Anwendungen im Gesundheitswesen“ definiert. Diese Sicherheitsanforderungen wurden basierend auf den Erfahrungen, welche bei der Durchführung explorativer Projekte im Gesundheitswesen unter Beteiligung der Industrie gewonnen wurden, erarbeitet. Darüber hinaus sind sie in Kooperation mit dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) formuliert und Ende Q2 2022 auf der Homepage des BSI veröffentlicht worden.

2.3 Digitale Pandemiebekämpfung

Im Frühjahr 2020 wurde der Gesellschaft mit dem Beginn der Corona-Pandemie ruckartig der Stecker gezogen. Der Alltag vieler Menschen wurde jäh ausgebremst und die Bürgerinnen und Bürger in Deutschland zogen sich in die eigenen vier Wände zurück. Dieses Verhalten war aufgrund der allgemeinen Sorge um eine Ansteckung mit Covid-19 nachvollziehbar. Um den Bürgerinnen und Bürgern wieder ein möglichst „normales“ Leben zu ermöglichen, begannen noch im selben Jahr die Bestrebungen, mittels technischer Hilfsmittel die Einschränkungen der Corona-Pandemie zu begrenzen. Im Mittelpunkt standen dabei Apps zur Kontaktverfolgung bei einer Infektion und für den einfachen Nachweis einer Immunisierung.

Abbildung 4: Corona-Warn-App Logo

Quelle: https://www.coronawarn.app/de/

2.3.1 Corona-Warn-App

Seit Beginn der Corona-Pandemie im März 2020 unterstützt das BSI die Entwicklung einer deutschen Covid-19-App. Das Ziel einer solchen Covid-19-App war es Menschen, welche bisher keine Anzeichen einer Covid-19-Infektion aufweisen, so schnell wie möglich darüber zu informieren, dass sie über einen längeren Zeitraum Kontakt mit einer infizierten Person hatten. Hierfür wurde eine Entfernungsmessung basierend auf der Bluetooth Low Energie-Technologie entwickelt.

Bei der Entwicklung einer Covid-19-App kristallisierten sich zwei unterschiedliche Ansätze heraus. Der erste lag in der Umsetzung eines zentralen Systems unter dem Namen „Pan-European Privacy-Preserving Proximity Tracing“ (PEPP-PT). Bei diesem Ansatz wurden bereits bei frühen Versionen des Sicherheitskonzeptes fortschrittliche Ansätze zur Anonymisierung der Nutzer berücksichtigt. Das BSI unterstützte die Fortentwicklung durch kontinuierliche Sicherheitsberatung, Penetrationstests und Quelltextanalysen von PEPP-PT. Im weiteren Verlauf des Projektes wurde ein alternativer, dezentraler Ansatz vorgestellt. Per Design ermöglichte dieser alternative Ansatz eine abgesicherte Anonymisierung und Freiwilligkeit, denn die Risikoermittlung für den Kontakt mit einer infizierten Person erfolgt durch das Mitführen des Endgerätes und die Operationen erfolgen ebenfalls auf dem Endgerät des Nutzers. Dieser Ansatz entwickelte sich später zu „Decentralized Privacy-Preserving Proximity Tracing“ (DP^3T) und bildete die Grundlage für die heutige Corona-Warn-App (CWA). Einen Meilenstein in der Entwicklung dieses Ansatzes war die Veröffentlichung des Exposure Notification Framework von Google und Apple. Hierdurch konnte die Entfernungsmessung mit Hilfe der in den Endgeräten verbauten Bluetooth Low Energie-Technologie, einheitlich implementiert werden.

Ende April beschloss die Bundesregierung den PEPP-PT Ansatz nicht weiter zu verfolgen. Stattdessen wurde ein Konsortium aus Telekom und SAP damit beauftragt einen dezentralen Ansatz auf Grundlage der Prinzipien aus DP^3T unter dem Namen Corona-Warn-App (CWA) für Deutschland zu entwickeln. Anlass war unter anderem ein Artikel des Chaos Computer Club, welcher Schwachstellen in der Anonymisierung unter der Annahme eines korrupten Backend-Betreibers identifizierte. Solche Schwachstellen sind beim DP^3T-Ansatz per Design nicht möglich.

Seit Beginn der Arbeiten an der Corona-Warn-App führt das BSI, ergänzend zum Entwicklungsprozess, Sicherheitsanalysen durch. Das BSI unterstützt die ständige Weiterentwicklung der Corona-Warn-App durch siebentägige Penetrationstests und Code-Reviews, welche bis Mitte 2022 in einem zweiwöchigen und seither in einem vierwöchigen Rhythmus stattfinden. Neben den erwähnten Reviews und Tests wurden auch die Sicherheitskonzepte der Anwendung durch das BSI analysiert. Zusätzlich wird der Quelltext der Corona-Warn-App transparent in einem öffentlich zugänglichen Quellcode-Verwaltungs-System (GitHub) veröffentlicht, worüber das BSI ebenfalls transparent identifizierte Schwachstellen an die Entwickler meldet.

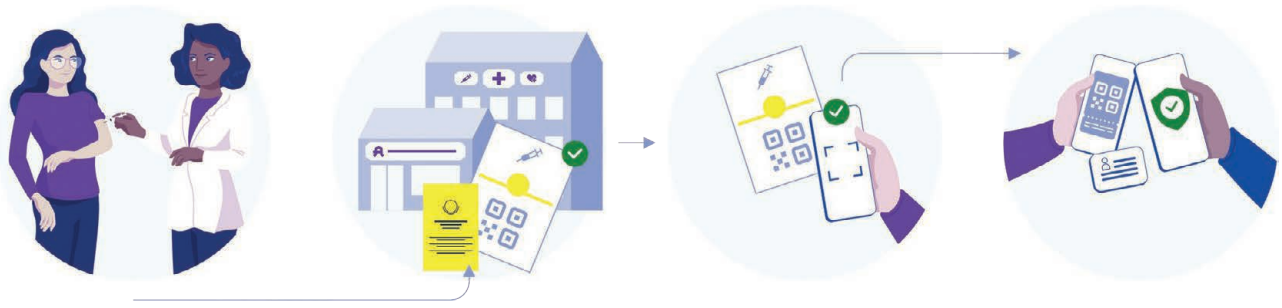
Seit der Veröffentlichung der Corona-Warn-App wurde diese in enger Zusammenarbeit zwischen BSI, RKI, Deutscher Telekom AG und SAP stetig weiterentwickelt und um zusätzliche Funktionalitäten ergänzt. Zu den wichtigsten Funktionserweiterungen gehören unter anderem die im Oktober 2020 mit Version 1.5 eingeführte Anbindung an den European Federal Gateway Service (EFGS). Durch diese Anbindung wurde die Kompatibilität der deutschen Corona-Warn-App mit anderen europäischen Corona-Apps hergestellt und Länderübergreifendes Tracing ermöglicht. Mit dem Update auf die Version 2.0.3 im April 2021 wurde die Corona-Warn-App um die Funktionalität der Eventregistrierung erweitert. Damit können Nutzerinnen und Nutzer im Einzelhandel, bei Veranstaltungen oder privaten Treffen per QR-Code einchecken, um mögliche Cluster und Infektionsketten zielgerichtet erkennen und unterbrechen zu können. Nachdem im Mai 2021 mit der Version 2.1.2 die Möglichkeit geschaffen wurde, die Ergebnisse von Schnelltests in der Corona-Warn-App anzuzeigen, konnte ab Juni 2021 mit der Version 2.3.2 der Impfstatus durch die Implementierung des digitalen Impfnachweises vorgezeigt werden. Durch diese und weitere Funktionserweiterungen wurden die Nutzerinnen und Nutzer in die Lage versetzt, Informationen und Funktionen rund um das Corona-Virus in einer einzigen Anwendung zu verwalten.

Dank der engen Zusammenarbeit mit dem BSI und der Transparenz gegenüber der Bevölkerung ist die Corona-Warn-App eine der sichersten und datenschutzfreundlichsten mobilen Applikationen in den App-Stores.

2.3.2 Digitaler Impfnachweis

Mit dem digitalen Impfnachweis hat die Bundesregierung für jede Bürgerin und jeden Bürger ab Juni 2021 eine Möglichkeit geschaffen, unkompliziert den eigenen Impfstatus nachzuweisen. Damit Bürgerinnen und Bürger ohne große Probleme ihre persönlichen Zertifikate erhalten können, musste eine komplett neue Infrastruktur geschaffen werden. Dazu gehörten nicht nur die Ausgabeorte (Arztpraxen, Apotheken, Impfzentren) der digitalen Nachweise, sondern insbesondere auch die IT-Systeme im Hintergrund.

Abbildung 5: Ablauf Import des digitalen Impfzertifikates



Quelle: www.digitaler-impfnachweis-app.de (letzter Zugriff 10.11.2022)

2.3.2.1 Was ist der digitale Impfnachweis?

Nach der COVID-Impfung erhalten alle Bürgerinnen und Bürger den klassischen Eintrag in das gelbe Impfheft. Dies entspricht der klassischen, analogen Dokumentation von Impfungen. Zusätzlich wird ein digitales EU-COVID-Impfzertifikat inklusive zugehörigem QR-Code ausgestellt. Der digitale EU-COVID-Impfausweis kann auch nachträglich in der Apotheke oder beim örtlichen Gesundheitsamt gegen Vorlage des gelben Impfbuchs ausgestellt werden. Um das digitale Zertifikat komfortabel auf dem Smartphone griffbereit zu haben, scannt die Bürgerin oder der Bürger den QR-Code mit der CovPass-App und fügt so das digitale EU Impfzertifikat ihrer oder seiner persönlichen CovPass-App hinzu. Mit den im Smartphone abgelegten Informationen, die durch einen QR-Code repräsentiert und für die CovPassCheck-App lesbar sind, kann das digitale Impfzertifikat beim Betreten von Veranstaltungen, Hotels oder Restaurants mit der CovPassCheck-App gescannt und überprüft werden. So muss lediglich das persönliche Smartphone und ein Ausweisdokument mitführt werden, um seinen individuellen Impfstatus sicher nachweisen zu können.

Abbildung 6: Zusammenspiel CovPass- und CovPass-Check-App

Quelle: www.digitaler-impfnachweis-app.de (letzter Zugriff: 10.11.2022)

Aufgrund eines kompatiblen Datenformats und dem Austausch mit einem von der EU betriebenen Zertifikatsserver sind die in Deutschland ausgestellten digitalen Impfzertifikate in der kompletten EU gültig. Dies gilt natürlich auch umgekehrt für in anderen EU-Ländern ausgestellte Zertifikate bei der Überprüfung mit der CovPassCheck-App. Darüber hinaus ist das EU-COVID-Impfzertifikat sogar in einigen Nicht-EU-Ländern für dort eingesetzte Check-Apps lesbar. Dabei ist diese Lösung sowohl besonders sicher als auch datenschutzfreundlich und datensparsam.

- Der QR-Code ist kryptografisch signiert, so dass die Überprüfung mit der CovPassCheck-App sofort erkennt, wenn das Impfzertifikat gefälscht ist.

- Jegliche Kommunikation ist verschlüsselt. Egal, ob Datenaustausch zwischen Hintergrundsystemen der CovPass-App stattfindet oder mit europäischen Servern kommuniziert wird.

- Für den QR-Code wurde ein europaeinheitlicher minimaler Datensatz definiert, der so wenige Daten wie möglich enthält. Somit erhalten Prüfende nur die Informationen über andere Bürgerinnen und Bürger, die notwendig sind, um den gültigen Impfstatus verifizieren zu können. Es erfolgt keine Speicherung von Daten in der Prüf-App.

- Um kein attraktives Ziel für Angriffe darzustellen, werden keine Daten zentral vorgehalten. Auf den Servern des Robert-Koch-Instituts (RKI), auf denen die digitalen Impfzertifikate erzeugt werden, geschieht dies lediglich temporär im Arbeitsspeicher. Dieser wird anschließend wieder freigegeben und die darin enthaltenden Daten gelöscht, so dass keine Daten dauerhaft gespeichert werden.

2.3.2.2 Wie ist der digitale Impfnachweis technisch realisiert?

Bei dem QR-Code handelt es sich um ein CBOR Web Token (CWT), das neben dem eigentlichen Zertifikat auch die notwendigen persönlichen Daten des Zertifikatsinhabers enthält. Dies sind lediglich der Name, das Geburtsdatum und die Informationen zur Impfung. Um eine einheitliche Lösung für die EU zu ermöglichen, wurde die Struktur durch eine Richtlinie der eHealth-Gruppe der EU definiert. Diese sieht außerdem vor, dass Integrität und Authentizität dieser Daten mittels CovPassCheck-App nachprüfbar sind. Um diesen Mechanismus bereitzustellen, wird der CWT mit einem asymmetrischen elektronischen Signaturverfahren signiert. Um den europaweiten Einsatz zu gewährleisten, stellen die Mitgliedsländer die zugehörigen öffentlichen Schlüssel auf einem zentralen EU-Server zur Verfügung. So verfügen alle teilnehmenden Staaten stets über die aktuellen Signaturdaten.

Weitere Details zur in der EU konsolidierten technischen Umsetzung

2.3.2.3 Wie sieht die Beteiligung des BSI aus?

Das BSI wurde vom Bundesministerium für Gesundheit (BMG) gebeten, die sicherheitstechnische Betrachtung der deutschen Lösung des digitalen Impfnachweises zu übernehmen. Diese Arbeiten haben im Frühjahr 2021 damit begonnen, dass das BSI frühzeitig im Entwicklungsprozess Sicherheits- und Kryptokonzepte bewertet und freigegeben hat. Neben diesen initialen Tätigkeiten wurden sowohl die Hintergrundsysteme als auch jede Version der CovPass- und CovPassCheck-App umfangreichen Penetrationstests unterzogen. So konnten vor dem Release neuer Funktionen identifizierte Schwachstellen in Rücksprache mit den Entwicklern behoben werden.

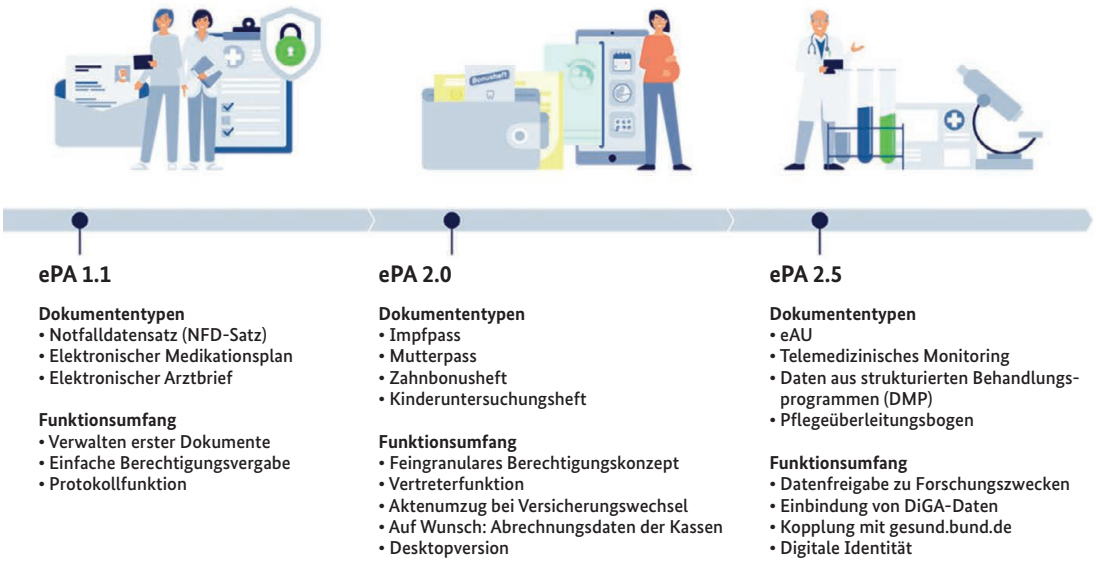
Durch regelmäßige und enge Abstimmung zwischen dem RKI, dem BMG, dem BSI und den beauftragten Entwicklern wurden die Konzepte, Hintergrundsysteme und Apps stets weiterentwickelt, so dass die dynamischen Vorgaben der EU, die im Laufe der Zeit hinzukamen, in der deutschen Lösung sicher und zeitnah umgesetzt wurden.

2.4 Ambulante Versorgung

Der schon vorhandene hohe Digitalisierungsgrad in der ambulanten Versorgung im deutschen Gesundheitswesen wird durch mehrere gesetzliche Vorgaben noch deutlich gesteigert.

Im Fokus dieser Digitalisierungsprojekte, beispielsweise des stufenweisen Ausbaus (siehe Abbildung 7) der schon eingeführten elektronischen Patientenakte und der bundesweiten Einführung des elektronischen Rezepts (E-Rezept) für alle gesetzlich Versicherten, steht der Ausbau des zentralen Netzwerks des Gesundheitswesens, der TI, durch die gematik GmbH. Mittlerweile ist fast jede Praxis durch ein lokales Netzkoppelelement (Konnektor), mit den zentralen Fachdiensten der gematik GmbH verbunden.

Abbildung 7: Dynamischer Ausbau der ePA



Quelle: gematik GmbH, https://www.gematik.de/anwendungen/e-patientenakte/ (letzter Zugriff: 10.11.2022)

Zusätzlich bedingen neue Anwendungen, wie zum Beispiel auch die „Kommunikation im Medizinwesen“ (KIM), die den Kommunikationsaustausch zwischen allen medizinisch tätigen Akteuren bestimmen soll oder die „elektronische Arbeitsunfähigkeitsbescheinigung“ (eAU), die das Meldewesen bei Erkrankungen vereinfachen soll, eine Vielzahl von Anforderungen an das Gesamtsystem, die durch die Software-Hersteller bis zu den Verwaltungssystemen in den Praxen zeitnah implementiert werden müssen.

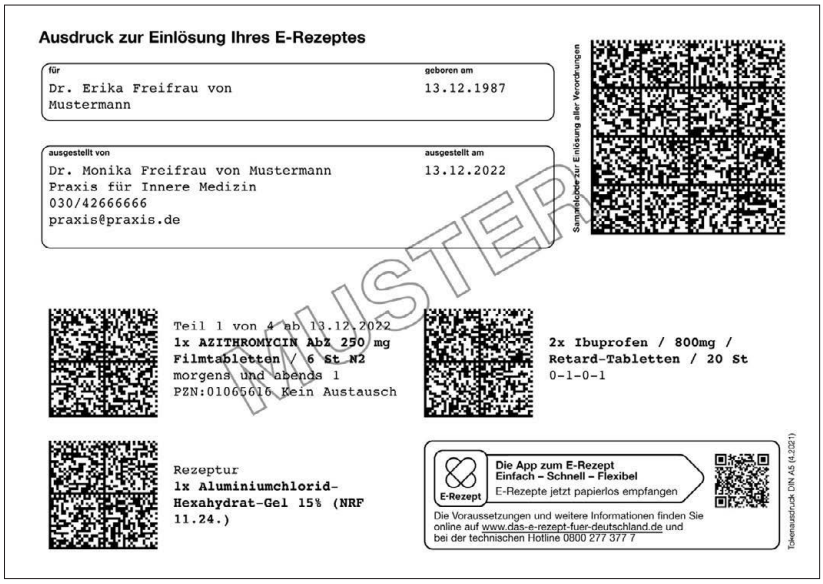
Es ist davon auszugehen, dass sich die zunehmende Digitalisierung zwangsläufig auf die notwendigen Kompetenzen der Leistungserbringer (Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Psychotherapeutinnen und Psychotherapeuten) zur Verarbeitung digitaler Informationen in den Praxen auswirkt und veränderte Voraussetzungen zur Diagnosestellung entstehen. Darüber hinaus wird sich ebenfalls der Anspruch der Versicherten an medizinische Leistungen wandeln, was beispielsweise zu einem gesteigerten

Wunsch nach digitalen Sprechstunden oder online-Buchung von Behandlungsterminen führt. Durch die Digitalisierung ist eine Verbindung zum Internet für den Betrieb der Praxisnetze oder vernetzte Geräte innerhalb der Praxis fast unumgänglich, sei es zum regelmäßigen Update der Systeme oder um Patientinnen und Patienten digitale Service- oder Dienstleistungen anzubieten.

Vor dem Hintergrund der Gewährleistung der Informationssicherheit mit den Grundwerten Vertraulichkeit, Authentizität und Integrität ist durch entsprechende Prozesse und technische Lösungen sicherzustellen, dass nur berechtigte Personen Zugriff auf die Daten haben, sie vor Änderung sowie Fälschung geschützt sind und ihr Ursprung nicht abgestritten werden kann.

Daher werden bei der Einbindung von Geräten in die Telematikinfrastruktur ausschließlich vom BSI zertifizierte Geräte, wie zum Beispiel das entsprechende Kartenlesegerät oder die eGK selbst (Kennzeichnung auf der rechten unteren Ecke der Karte), verwendet.

Abbildung 8: E-Rezept Muster



Quelle: KBV - Elektronisches Rezept (eRezept), https://www.kbv.de/media/sp/Ausdruck_Einloesung_eRezept_Freigabe__2021_04_21_web.pdf (letzter Zugriff: 10.11.2022)

Eine weitere digitalisierte Versorgung stellt das bereits erwähnte E-Rezept dar. Bisher werden jährlich rund 500 Millionen Rezepte analog für gesetzlich Versicherte ausgestellt. Seit September 2022 wird das E-Rezept bundesweit ausgerollt, so dass in Kürze alle Versicherten auf elektronischem Wege eine ärztliche Verordnung bekommen können sollten. Hierbei können Leistungserbringer mittels ihrer Praxis-Verwaltungssysteme (PVS) und der entsprechenden Verordnungssoftware der Patientin oder dem Patienten eine elektronische Verordnung ausstellen. Dazu wird der individuelle Heilberufsausweis (HBA) genutzt und die Verordnungsdaten über den Konnektor (ohne Fachlogik) in die TI übertragen. Über dieses gesicherte Netz wird der Verordnungsdatensatz verschlüsselt in den Fachdienst E-Rezept übertragen. Statt einer klassischen Ende-zu-Ende-Übertragung wird in der Prozesskette des Fachdienstes eine „vertrauenswürdige Anwendungs Umgebung“ (VAU) eingesetzt, welche ähnlich der bei der elektronischen Patientenakte eingesetzten Komponente, in Sekundenbruchteilen eine Umschlüsselung zum erweiterten Zugriffsschutz vornimmt.

Die Versicherten können über eine App (Frontend des Versicherten E-Rezept) mittels ihrer e-GK und PIN auf den Fachdienst zugreifen und dort den vollständigen E-Rezept-Dateneinsatz einsehen und zur Aushändigung in der Apotheke vorzeigen oder elektronisch einer Apotheke ihrer Wahl zuweisen.

2.5 Kritische Infrastrukturen

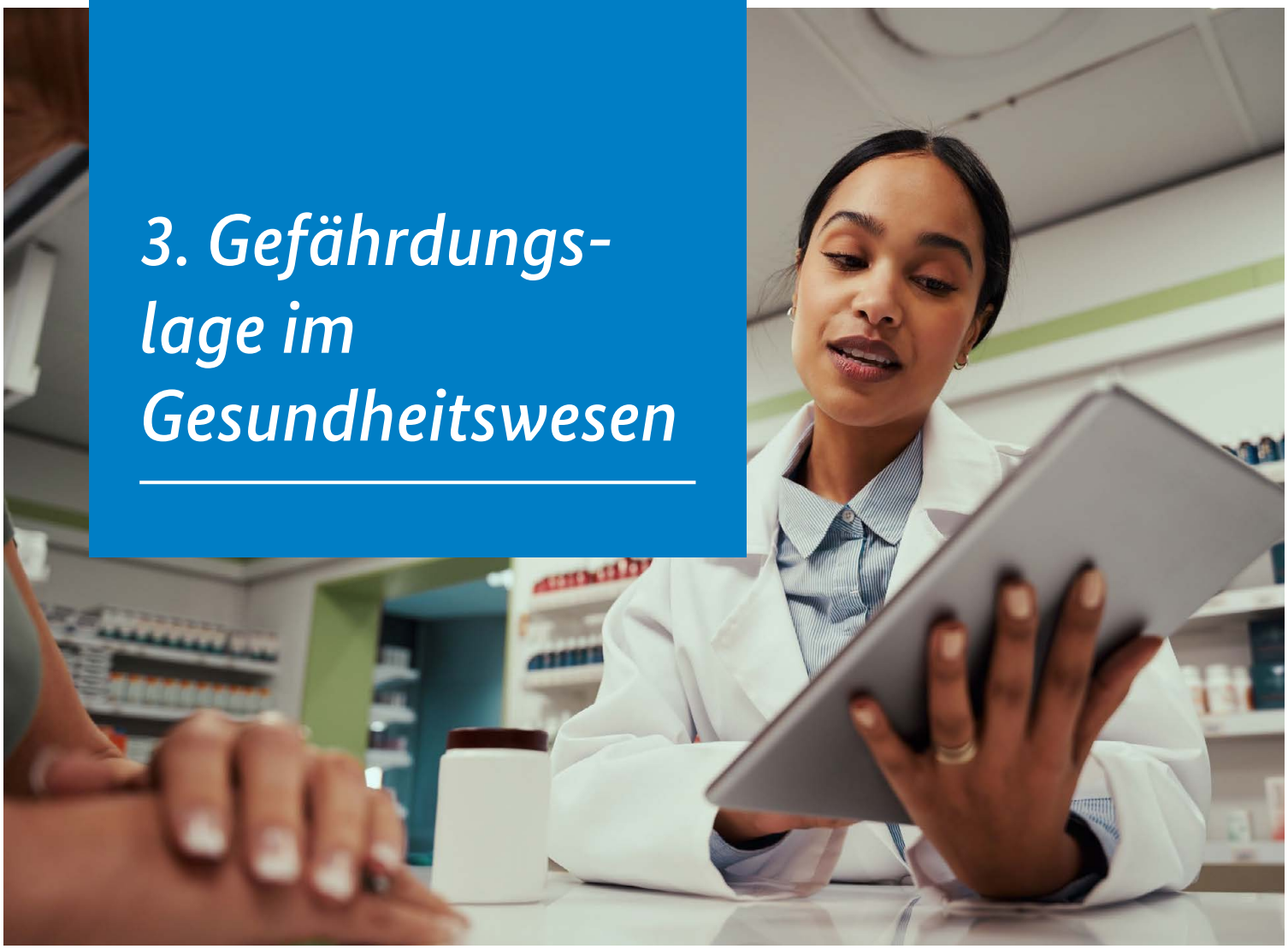
Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Gemäß § 2 Absatz 10 BSIG [4] sind Kritische Infrastrukturen im Sinne dieses Gesetzes Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

In Bezug auf ihre gesellschaftliche Bedeutung, tragen Krankenhäuser, Labore und viele andere Einrichtungen des Gesundheitswesens in mehrfacher Hinsicht eine besondere Verantwortung für ihre IT-Netze.

Die Kritische Dienstleistung erstreckt sich hierbei auf:
- die stationäre medizinische Versorgung,
- die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind,
- die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper,
- die Laboratoriumsdiagnostik.

Ausgehend von dieser Aufteilung, gibt es insgesamt 11 verschiedene Anlagenkategorien, die für die Regulierung der Kritischen Infrastruktur im Sektor relevant sind [5].

Der Schutz sensibler Patientendaten muss hierbei ebenso zuverlässig gewährleistet sein, wie die Versorgung von Patientinnen und Patienten mit Unterstützung modernster Computertechnologie. Öffentlich bekannt gewordene IT-Sicherheitsvorfälle zeigen, dass medizinische Einrichtungen gezielt und ungezielt Opfer eines Cyber-Angriffs werden können. Nicht zuletzt aufgrund der zunehmenden Digitalisierung im Bereich der medizinischen Versorgung stehen vor allem die Betreiber Kritischer Infrastrukturen, vermehrt vor großen Herausforderungen im Hinblick auf die Absicherung ihrer IT-Systeme, -Prozesse und -Komponenten. Eine Vielzahl von Betreibern fällt schon heute unter die Anforderungen aus dem BSI-Gesetz (BSIG) sowie der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) und weisen dem BSI bereits die Umsetzung von technischen und organisatorischen IT Sicherheitsmaßnahmen nach dem Stand der Technik nach. Doch auch für Betreiber unterhalb der jeweiligen Schwellenwerte aus der BSI-KritisV rückt IT-Sicherheit immer stärker in den Fokus. Diese Werte sind innerhalb der Verordnung für jeden Sektor und jede Branche nach festen Formeln definiert und beziehen sich beispielsweise bei Krankenhäusern auf die vollstationäre Fallzahl / Jahr (30.000 vollstationäre Fälle pro Jahr) oder im Hinblick auf die Labore auf die Anzahl der Aufträge / Jahr (1.500.000 Aufträge pro Jahr). Mehrere Gründe können dazu führen, dass ein Betreiber zum ersten Mal den geltenden Schwellenwert überschreitet und dadurch neu unter die Anforderungen aus dem BSIG und der BSI-KritisV fällt. In diesem Zusammenhang wird es auch zukünftig zwingend notwendig sein, dass die Betreiber aus dem Gesundheitssektor verstärkt den Prozess ihrer kritischen Dienstleistung analysieren, um diesen durch die Umsetzung von IT-Sicherheitsmaßnahmen bestmöglich schützen zu können.



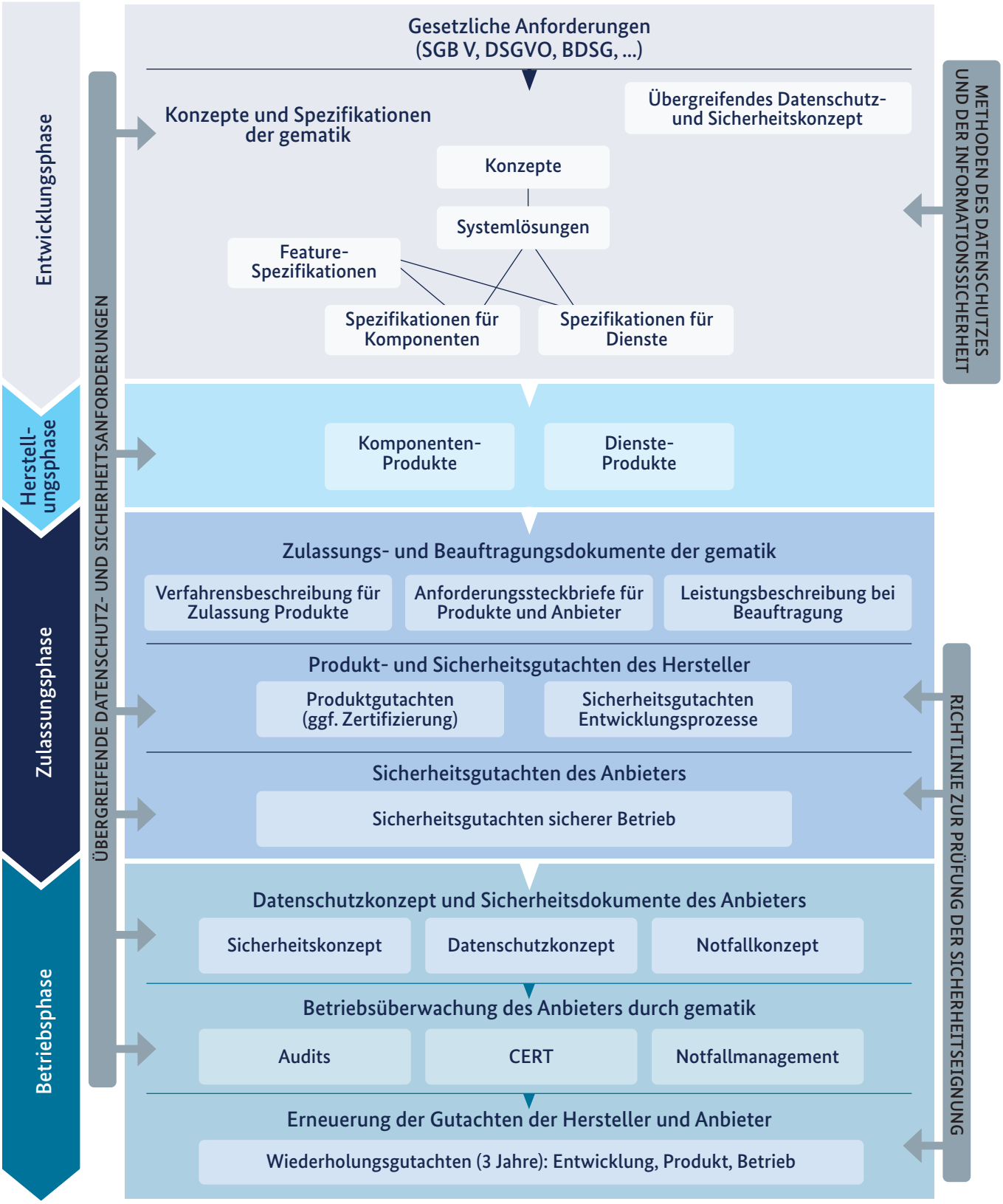
3. Gefährdungslage im Gesundheitswesen

3.1 Telematikinfrastruktur

Der Gefährdungslage in der Telematikinfrastruktur wird in einem mehrstufigen Prinzip begegnet. In erster Linie liegt die Realisierung der IT-Sicherheit bei den Herstellern und Betreibern der jeweiligen Dienste und Komponenten, bspw. KIM Fachmodul. Diese müssen ihre Sicherheitsvorkehrungen nach Vorgaben der gematik gestalten, wobei bei der Konzeption konkreter Sicherheitsvorgaben ein Einvernehmen mit dem BSI hergestellt wird, bei dem alle Sicherheitskonzepte und Spezifikationen vom BSI begutachtet und erst nach Zustimmung in Kraft gesetzt werden. Dienste und Komponenten unterliegen sowohl einem Zulassungsverfahren der gematik als auch einer sicherheitstechnischen Zertifizierung des BSI. Der laufende Betrieb wird durch das Cyber Emergency Response Team (CERT) der gematik überwacht und Sicherheitsvorfälle werden dem BSI gemeldet, so dass die Vorfallsbearbeitung in die Bewältigungsprozesse des Lagezentrums des BSI integriert werden. Diese komplexen Sicherheitsstrukturen sind erforderlich, um den hohen Anforderungen an den Schutz sensibler medizinischer Daten gerecht zu werden, zumal die Nutzung der TI gesetzlich vorgeschrieben ist. Neben dem BSI wird in Sicherheitsfragen auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) eng eingebunden.

Um Schwachstellen, die erst im laufenden Betrieb erkennbar sind, rechtzeitig zu erkennen, folgt die gematik einem Überwachungskonzept mit Maßnahmen zur Schwachstellenerkennung auf Ebene der Planungsphase, Build-Phase und Run-Phase. Diese Phasen umfassen gematik, Anbieter bzw. Betreiber und Entwickler. Die Abbildung 9 gibt einen Überblick über die Phasen und damit verbundenen Artefakte, die zu dieser „360°-Sicherheit“ führen.

Abbildung 9: Überblick der Artefakte in den Phasen des Lebenszyklus der TI



Inhalte: gematik GmbH, 2021

3.1.1 Konzepte und Spezifikationen

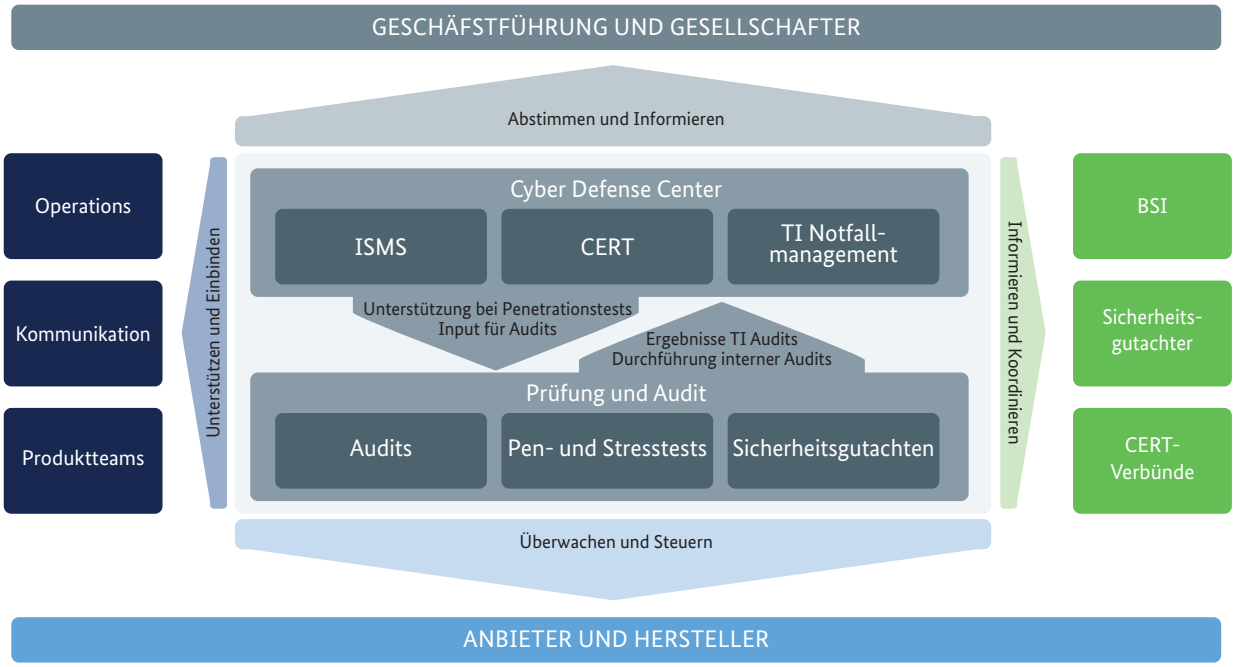
Die Vorgaben der gematik an Hersteller und Betreiber, aber teilweise auch an die gematik selbst oder an die Fachöffentlichkeit, werden in Konzepten und Spezifikationen definiert. Soweit hierbei die Sicherheit der Informationstechnik betroffen ist, muss zu den Dokumenten nach § 311 SGB V ein Einvernehmen mit dem BSI hergestellt werden, und soweit der Datenschutz betroffen ist mit dem BfDI. Faktisch ist die Erstellung dieser Dokumente ein eng getakteter Austausch zwischen der gematik und den Behörden, in dem das BSI insbesondere Wert darauflegt, den Stand der Technik in der IT-Sicherheit in die Dokumente einfließen zu lassen. Die Spezifikationen bieten wiederum die Grundlage für weitere zulassungsrelevante Vorgaben, wie die Vorgaben des BSI zum Prüfverfahren der Komponenten und Dienste und die Vorgaben zum Zulassungsverfahren der gematik, das sich auf Funktionalität, Operabilität und Betriebssicherheit fokussiert.

3.1.2 Zulassung, Prüfung, Audit und Zertifizierung

Dienste und Komponenten der Telematikinfrastruktur werden von der gematik geprüft und zugelassen, die auch die Verantwortung für den Betrieb trägt. Hierin sind je nach Bedarf auch Penetrationstests und Audits der Betreiber enthalten. Darüber hinaus werden Sicherheitszertifizierungen der Komponenten und Dienste gemäß § 325 SGB V nach Vorgaben des BSI vorgenommen – Hierzu veröffentlicht das BSI entsprechende Technische Richtlinien (bei TR-Zertifizierung) oder Protection Profiles (bei CC-Evaluation). Die Rechtsaufsicht und somit die Überwachung der Erfüllung gesetzlicher Pflichten liegt beim Bundesministerium für Gesundheit (BMG). Vorgaben zur Zulassung, den Überprüfungen und der Zertifizierung werden sowohl gematikseitig als auch BSI-seitig fortlaufend der fortschreitenden Telematikinfrastruktur und dem Stand der Technik angepasst. So liegt in den aktuellen Arbeiten des BSI ein Schwerpunkt auf mobilen Anwendungen wie den „Frontends des Versicherten“ (FdV) für ePA und E-Rezept. Hierbei müssen auch regulative Fortschritte in angrenzenden Gebieten berücksichtigt werden, wie beispielsweise im Bereich der digitalen Pflege- und Gesundheitsanwendungen. Aber auch „klassische“ Sicherheitszertifizierungen werden fortlaufend dem aktuellen Stand angepasst – So beispielsweise die Zertifizierung des Konnektors, seiner Fachmodule oder anderer Hardware-Komponenten.

Gegenüber den Herstellern und Betreibern gibt die gematik Sicherheitsvorgaben vor und überwacht deren Umsetzung. Die operativen Aufgaben hierzu werden von einem Cyber Defense Center wahrgenommen. Hierbei liegen Schwerpunkte auf an ISO 27001 orientierten Vorgaben zum Informations-Sicherheits-Management-System (ISMS), dem Betrieb eines Cyber-Emergency-Response-Teams (CERT) und einem Notfallmanagement. Die Prüfungen der betrieblichen Sicherheit umfassen Audits, Penetrations- und Stresstests und Sicherheitsgutachten (Siehe Abbildung 10).

Abbildung 10: Aufgabenschwerpunkte betriebliche Sicherheit der TI



Inhalte: gematik GmbH, 2021

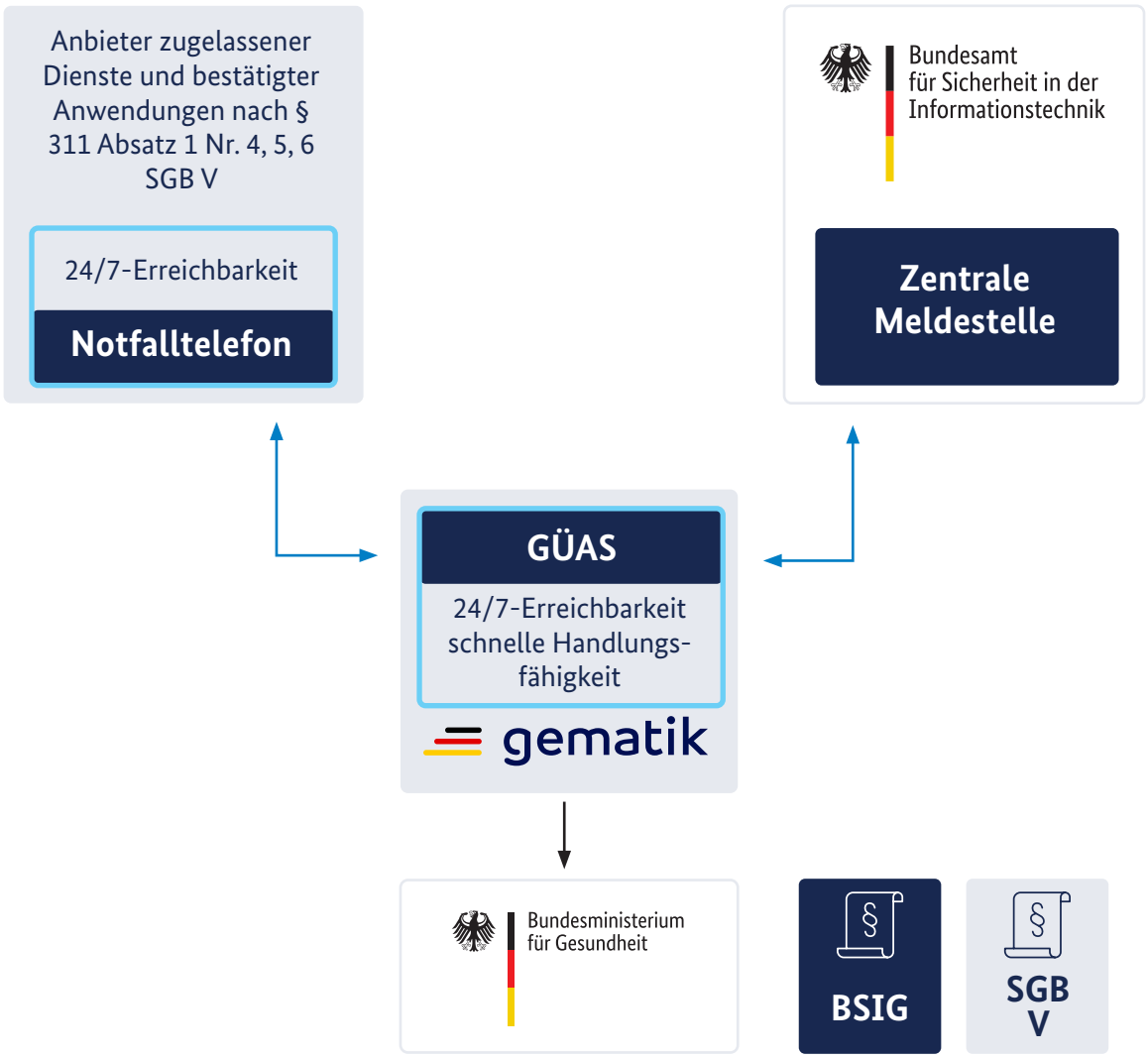
Das CERT des BSI wird als zentrale Meldestelle analog zum KRITIS-Bereich in die Vorfallsbearbeitung eingebunden: Vorfallsmeldungen werden dem BSI weitergeleitet und Maßnahmen werden, der jeweiligen Lage angebracht, zwischen BSI und gematik abgestimmt. Die gematik arbeitet dabei als gemeinsame übergeordnete Ansprechstelle (GÜAS) für die von ihr betreuten Betreiber (siehe Abbildung 11). Bisher handelte es sich bei den im CERT des BSI eingegangenen Meldungen überwiegend um Verfügbarkeitsmeldungen aufgrund technischer Defekte, so dass nur geringe Unterstützung des BSI angebracht war.

Das BSI kann nach § 333 SGB V aber auch verbindliche Anweisungen zur Beseitigung von Sicherheitsmängeln erteilen, so dass insbesondere bei schwerwiegenden Cyber-Sicherheitslagen und Krisen interveniert werden kann.

Die aktuelle Sicherheitslage der Telematikinfrastruktur wird durch die gematik im „TI-Status“ veröffentlicht. Hier wird transparent über aktuelle betriebliche Ereignisse und Störungen aufgeklärt.

Der Status kann auf folgender Website abgerufen werden.

Abbildung 11: Melde- und Anweisungsflüsse zu § 311 SGB V



Quelle: gematik GmbH, 2021, Entwurf: "Übergreifendes Datenschutz- und Sicherheitskonzept der TI 2.0"

3.1.3 Sicherheitsvorfälle und besondere Ereignisse

Die Anzahl an Sicherheitsvorfällen, die durch das CERT der gematik an das CERT des BSI gemeldet wurden, ist sehr gering. Dies ist ein deutlicher Hinweis darauf, dass die getroffenen Sicherheitsmaßnahmen und -prozesse wirksam sind. Im Zeitraum Juli 2021 bis Oktober 2022 wurden sechs Vorfälle gemeldet. Hierbei bezog sich ein Vorfall auf einen Angriff auf einen Dienstanbieter der Telematikinfrastruktur, wobei sich herausstellte, dass die TI selbst nicht betroffen war. Bei zwei Vorfällen waren die Anbieter von Diensten durch DDoS Angriffe für Stunden teilweise gestört, sodass es zu Timeouts oder einer Limitierung der gleichzeitig möglichen Zugriffe kam. Es kam zu drei Ausfällen durch technischen Defekt oder Fehlkonfiguration über mehrere Stunden, einer davon sogar länger als einen Tag. Die Anzahl von Betroffenen variierte bei diesen Vorfällen, sodass bei einem Ausfall zwischen 250.000 und 500.000 mögliche Betroffene geschätzt wurden, ansonsten weniger als 250.000 (dem kleinsten bei Vorfallsmeldungen wählbaren Wert).

Im August 2022 wurde durch den Chaos Computer Club (CCC) eine Dokumentation von Angriffsvektoren auf die Video- und Autoidentifizierungsverfahren publiziert. Gemäß Angabe konnte der CCC die Verfahren von sechs VideoIdent-Anbietern aushebeln und dabei beispielsweise eine elektronische Patientenakte anlegen und befüllen. Weitergehend war es möglich auf die Daten aus der Akte einer eingeweihten Testperson zuzugreifen. Als Reaktion hierauf hat die gematik die weitere Nutzung von VideoIdent-Verfahren für die Ausgabe von Identifizierungsmitteln zur Nutzung in der TI bis zur Schließung der Lücken als nicht mehr zulässig erklärt und am 09.08.2022 verfügt, dass die Krankenkassen das VideoIdent-Verfahren ab sofort aussetzen. Die vom CCC beschriebenen Angriffsvektoren stellen nicht nur eine Bedrohung für das Gesundheitswesen dar, sondern haben potenziell auch auf weitere Branchen Auswirkungen.

3.2 Medizinprodukte

In vielen Bereichen gewährleisten Medizinprodukte autonom lebenserhaltende Funktionen. Aus diesem Grund ist es notwendig, dass sie eine hohe Ausfallsicherheit und Stabilität aufweisen. Kleinste Abweichungen in ihrer Grundfunktionalität können bereits schwerwiegende Folgen für die Patientensicherheit bedeuten. Im Rahmen der Digitalisierung und Vernetzung besteht zusätzlich zu normalen Fehlfunktionen mit vielfältigen Ursachen zunehmend eine mögliche Bedrohung durch digitale Cyber-Angriffe und Manipulation aus der Ferne. Außerdem kommen durch die Digitalisierung neue Maßnahmen zur Erhebung und Verwaltung von Gesundheitsdaten zum Einsatz, die als Grundlage von medizinischen Behandlungen dienen. Durch diesen Hintergrund stellen Angriffe auf die Vertraulichkeit und Integrität der Gesundheitsdaten einen zusätzlichen Faktor dar.

3.2.1 Vernetzung von Medizinprodukten

Trotz vieler Vorteile durch „smarte“ Funktionen bringen vernetzte Medizinprodukte auch Nachteile im Bereich der Cyber-Sicherheit mit sich: Durch den Einbau von digitalen Schnittstellen und insbesondere der Anbindung der Medizinprodukte an weitere Geräte und Netzwerke wird auch die Angriffsfläche vergrößert, wie in Abbildung 3 durch die rot markierten angreifbaren Verbindungen dargestellt ist. Bei analogen Medizinprodukten gibt es lediglich die Risiken, dass ein Gerät physisch in seinem Betrieb gestört oder manipuliert werden kann. Bei vernetzten Geräten besteht hingegen zusätzlich die Möglichkeit einer Kompromittierung aus der Ferne. So konnte im letzten Jahr bei einer vernetzten Spritzenpumpe, die im Krankenhaus und im Rettungsdienst zum Einsatz kommt, eine Sicherheitslücke entdeckt werden, die einem Angreifer aus der Ferne die Manipulation der Kalibrierung zur Medikamentendosierung erlaubte. Dadurch konnte

die mangelhafte Cyber-Sicherheit potentiell auch die Patientensicherheit gefährden. Glücklicherweise wurde die Lücke vor einer potentiellen Ausnutzung geschlossen und keine zu behandelnde Person ist zu Schaden gekommen. Allerdings tritt ein Fall wie dieser nach den Erfahrungen des BSI nur sehr selten auf. Im Rahmen der Projekte ManiMed [6] und eCare [7] hat das BSI gezeigt, dass die meisten vernetzten Medizinprodukte eine hohe Patientensicherheit gewährleisten und die gefundenen IT-Schwachstellen keine gravierende Bedrohung darstellen. Doch über das reine Patientenrisiko hinaus kann auch das Risiko bestehen, dass Gesundheitsdaten, die besonders schützenswert sind, durch Angreifer erlangt werden und in fremde Hände geraten. Jede zusätzliche Schnittstelle stellt eine potentielle Bedrohung dar und in jeder Software gibt es ausnutzbare Schwachstellen. Diese werden teilweise auch erst Jahre nach der Markteinführung eines Geräts entdeckt. Aus diesem Grund ist eine stetige Beobachtung und Lieferung von Sicherheitsupdates notwendig und viele Hersteller veröffentlichen eigenständig gefundene Sicherheitslücken, sodass Betreiber ein Patientenrisiko frühzeitig vermeiden können. Bei einigen vernetzten Medizinprodukten, insbesondere bei stationären Geräten, kommt es allerdings vor, dass ein Hersteller zusätzliche Software- und Hardware-Komponenten von Drittanbietern einsetzt und selbst keine Kenntnisse über darin eventuell vorhandene Sicherheitslücken hat. Zu diesem Zweck ist ein neuer Ansatz in Planung, bei dem jeder Lieferant alle eingesetzten Softwarekomponenten inklusive ihrer Version ähnlich einer Zutatenliste genau benennen muss. Das erlaubt in Zukunft, dass sofort ersichtlich ist, welches Gerät von einer bestimmten Sicherheitslücke betroffen ist. Dieser neue Überblick vereinfacht die gezielte Schließung von Sicherheitslücken in vernetzten Medizinprodukten. Dies ist ein bedeutender Schritt, da zunehmend mehr Medizinprodukte vernetzt werden und ein gutes Schutzniveau essentiell für das Gesundheitswesen ist.

Das BSI ist der zentrale behördliche Ansprechpartner zur Gewährleistung der Cyber-Sicherheit in vernetzten Medizinprodukten in Deutschland und zeigt sich verantwortlich für die Bewertung von neu gefundenen Schwachstellen nach § 85 MPDG und verfasst Leitfäden und technische Richtlinien zur Prävention von Sicherheitsvorfällen. Außerdem werden Projekte mit Produkttests durchgeführt und damit der gegenwärtige Zustand der Cyber-Sicherheit von Produkten auf dem Markt ermittelt sowie Hersteller und Betreiber sensibilisiert.

3.2.2 Digitale Gesundheits- und Pflegeanwendungen

Wie bereits erwähnt, ist im Gesundheitswesen die Vertraulichkeit von Daten, die unwillentlich offenbart werden, für immer verloren. Die betroffene Person könnte hierfür zwar Schadensersatz erhalten, die unwillentliche Offenbarung kann allerdings nicht revidiert werden. Durch das ungewollte Bekanntwerden von Gesundheitsdaten können im sozialen, wie auch im beruflichen Umfeld, unerwünschte Folgen mit erheblichen Auswirkungen entstehen. Sollte ein Angreifer darüber hinaus in der Lage sein, sensible Daten eines Dritten zu manipulieren und damit deren Integrität verletzen, könnte er wesentlichen Einfluss auf Therapieentscheidungen und letztlich auf die Gesundheit der betroffenen Person haben. Besonders vor dem Hintergrund dieser Schadensszenarien im Kontext digitaler Anwendungen im Gesundheitswesen ist das Einhalten von geeigneten Sicherheitsstandards im Gesundheitswesen von besonderer Relevanz.

Der Start von digitalen Gesundheitsanwendungen im Jahr 2020 hat jedoch gezeigt, dass geeignete Sicherheitsstandards von Herstellern nicht in allen Fällen berücksichtigt werden. Presseberichten zur Folgen fanden die Sicherheitsforscher Martin Tschirsich und André Zilch heraus, dass bereits eine der ersten DiGA triviale Sicherheitslücken aufwies [8]. So war es beispielsweise möglich über die Funktion zum Zurücksetzen des Passwortes Konten von anderen Patienten zu übernehmen. Hierbei wurde ein vierstelliger Code, welcher eine Gültigkeitsdauer von 24 Stunden besaß, an die hinterlegte E-Mail-Adresse versandt. Durch

Brute-Force-Angriffe konnte dieser dann erraten werden und E-Mail-Adressen und Nutzernamen von registrierten Nutzern ließen sich ohne Authentifizierung über einfache API-Calls abrufen.

In 2022 hat das Kollektiv „Zerforschung“ wenige ins Verzeichnis aufgenommene DiGAs betrachtet. Diese Betrachtung verdeutlicht, dass durchaus weiterer Handlungsbedarf besteht und verbindliche Sicherheitsstandards hierfür hilfreich sind. Laut Aussage des Kollektives weisen die wenigen digitalen Gesundheitsanwendungen, die sich das Kollektiv angeschaut hat, einen massiven Datenabfluss auf. „Insgesamt seien Daten von mehr als 20.000 Patientinnen und Patienten verloren gegangen“ [9]. Auch im Fall der von Zerforschung aufgedeckten Sicherheitslücken handelt es sich um eher triviale Schwachstellen. Der API-Call einer DiGA für den Abruf von personenbezogen Daten beispielsweise war hier zwar nicht möglich ohne sich als Patient zu authentifizieren, jedoch konnten nach erfolgreicher Authentifizierung Daten von allen Patienten abgerufen werden. Hierzu musste lediglich durch die 5-stellige fortlaufende User-ID iteriert werden.

Die Untersuchungen der Sicherheitsforschenden zeigen die Notwendigkeit von Sicherheitsstandards im Gesundheitswesen. Alle aufgedeckten Schwachstellen hätten durch eine Zertifizierung nach BSI TR 03161 „Anforderungen an Anwendungen im Gesundheitswesen“ verhindert werden können.

3.3 Digitale Pandemiebekämpfung

Durch die Entscheidung, die Corona-Pandemie auch mit digitalen Mitteln zu bekämpfen, entstand auch die Notwendigkeit, sich mit den damit einhergehenden Problemen auseinanderzusetzen. So sind mobile Anwendungen und deren Hintergrundsysteme natürlich Cyber-Sicherheitsrisiken ausgesetzt. Da es sich bei den Apps zur Pandemiebekämpfung im weiteren Sinne um Gesundheitsapps handelt, sind die vorliegenden Daten besonders schützenswert. Daher waren Security- und Privacy-by-Design im Entwicklungsprozess besonders relevant. Auch durch das zielgerichtete Mitwirken der Open-Source-Community konnte das BSI bei der Ausarbeitung von Konzepten und der Umsetzung der Anwendung diesen beiden Prinzipien und deren Bedeutung gerecht werden.

3.3.1 Corona-Warn-App

Seit Beginn der Arbeiten an der Corona-Warn-App führt das BSI, ergänzend zum Entwicklungsprozess, Sicherheitsanalysen durch. Seit der Veröffentlichung der Corona-Warn-App wurden in enger Zusammenarbeit, wie bereits in Kapitel 2.3.1 zwischen BSI, RKI, Deutscher Telekom AG und SAP diverse Erweiterungen veröffentlicht. Außerdem wurde eine Anbindung an das europäische Gesamtsystem sowie der Schweiz realisiert. Die genannten Erweiterungen erhöhen den Funktionsumfang der CWA und beheben identifizierte Schwachstellen. Durch die Aktivtäten des BSI wurden bisher über 80 Schwachstellen in der Corona-Warn-App identifiziert und mitigiert.

Zu den schwerwiegendsten Schwachstellen gehörten unter anderem:

- Remote Code Execution
- SQL-Injection
- Cross-Site Request Forgery

Die Remote Code Execution wurde von einem Mitglied des GitHub Security Labs gemeldet und an die Deutsche Telekom AG, SAP und das BSI übermittelt. Dies unterstreicht noch einmal die Wichtigkeit des transparenten Entwicklungsprozesses in einem öffentlich zugänglichen Quellcode-Verwaltungssystem. Die Schwachstelle ermöglichte das Übermitteln und Ausführen von Schadsoftware über das Internet im Submission-Server der Corona-Warn-App. Hierdurch wäre theoretisch eine komplette Übernahme der Hintergrundsysteme der Corona-Warn-App möglich gewesen. Ein Auflösen der Anonymisierung war jedoch zu keinem Zeitpunkt möglich. Aufgrund der

guten Zusammenarbeit zwischen dem Konsortium und dem BSI konnte die Schwachstelle innerhalb von drei Tagen nach Bekanntwerden geschlossen werden. Die Möglichkeit für eine SQL Injection konnte während des Penetrationstests durch das BSI identifiziert werden. SQL Injection Schwachstellen treten auf, wenn Daten unter der Kontrolle des Nutzers ungeprüft in Datenbankabfragen übernommen werden. Ein Angreifer wird so in die Lage versetzt durch manipulierte Eingabewerte Datenbankbefehle an das Hintergrundsystem zu übermitteln. Je nach Rechten des Nutzers ist so ein Abfluss von Informationen oder sogar die komplette Manipulation der Datenbank möglich. Durch die frühzeitige Beteiligung des BSI an der Entwicklung der Anwendung, konnte verhindert werden, dass diese Schwachstelle in den produktiven Betrieb gegangen ist.

Im Rahmen der Penetrationstests des BSI konnte ebenfalls eine Anfälligkeit für Cross-Site Request Forgery-Angriffe festgestellt werden. Hierbei wird ausgenutzt, dass viele Browser Berechtigungsnachweise (z.B. Session Cookies) in Anfragen automatisch mit der angefragten Seite in Verbindung bringt. Dadurch kann die Anwendung nicht zwischen gefälschten und berechtigten Anfragen unterscheiden. Angreifer nutzen dies üblicherweise bei Anfragen aus, die einen Status des Opfers ändern, z.B. Änderung des Passwortes. Der Angriff kann initiiert werden, indem dem Opfer eine URL zugesendet wird. Das Verwenden dieser URL bewirkt, dass der Empfänger die Aktion als legitime Anfrage des Nutzers interpretiert. In diesem konkreten Fall konnten TeleTANs im Namen eines angemeldeten Nutzers generiert werden. Die Schwachstelle konnte identifiziert und mitigiert werden bevor die Corona-Warn-App produktiv verwendet wurde.

Die Corona-Warn-App ist ein wichtiger Baustein der digitalen Pandemiebekämpfung. Gemeinsam mit dem Konsortium sorgt das BSI dafür, dass eine sichere und verlässliche Lösung für alle Bürgerinnen und Bürger zur Verfügung steht. Die Zusammenarbeit der Partner hat sich bisher sehr konstruktiv, effizient und vertrauensvoll gestaltet, sodass auch die weiteren Entwicklungen der Corona-Warn-App in diesem Modus bestritten werden können.

3.3.2 Digitaler Impfnachweis

Um ein möglichst hohes Maß an Sicherheit für den digitalen Impfnachweis zu erreichen, wurden Sicherheits- und Kryptokonzepte durch das BSI von Beginn an geprüft. So konnte eine solide theoretische Grundlage für die IT-Sicherheit des Gesamtsystems geschaffen werden. Neben technischen Maßnahmen wurden so auch organisatorische Maßnahmen, wie beispielsweise umfangreiche Zertifizierungen von Rechenzentren, in denen die Hintergrundsysteme betrieben werden, festgelegt.

Zusätzlich zu diesen theoretischen Grundlagen wurde jede neue Version der CovPass-Apps mindestens eine Woche lang durch erfahrene Penetrationstester untersucht. Diese Untersuchung hat neben den Apps auch die zugehörigen Hintergrundsysteme umfasst, so dass eine Vielzahl von Schwachstellen vor der Veröffentlichung einer neuen Version erkannt und behoben werden konnten.

Obwohl obengenannte Maßnahmen seit dem Projektstart berücksichtigt wurden, gab es immer wieder Fälle, in denen gefälschte oder unberechtigte Impfzertifikate zum Einsatz kamen. Diese Impfnachweise waren nicht aus technischer Sicht gefälscht, jedoch ließen diese Angriffe erkennen, wie komplex das Gesamtsystem „digitaler Impfnachweis“ und dessen Prozesse sind. So wurden beispielsweise digitale Nachweise durch grundsätzlich berechtigte Personen (wie zum Beispiel Apothekerinnen oder Ärzten) erstellt, jedoch nicht auf Grundlage einer tatsächlichen Impfung.

Eine andere Form der unberechtigten Impfzertifikate waren QR-Codes, die für den menschlichen Betrachter valide aussahen, jedoch keiner Überprüfung durch die europäischen Check-Apps standgehalten hätten.

Wenn prüfende Stellen (Veranstalter, Hotels, Gastronomen) alle Prüfschritte, d.h. Scannen des QR-Codes mittels CovPassCheck-App und Abgleich mit dem vorgelegten Ausweisdokument, gewissenhaft durchführen, ist die Gefahr mit gefälschten oder kopierten Impfnachweisen unberechtigten Zutritt zu erlangen sehr unwahrscheinlich. Lediglich die ungerechtfertigte Ausstellung von Zertifikaten durch autorisierte Personen stellt ein Restrisiko dar, jedoch ist es schlicht kaum möglich dies mittels technischer Vorkehrungen zu verhindern.

3.4 Ambulante Versorgung

Für den ambulanten Bereich der ärztlichen und zahnärztlichen Versorgung sind zahlreiche Erweiterungen durch fortschreitende Digitalisierung, insbesondere innerhalb der Telematikinfrastruktur des Gesundheitswesens wirksam geworden.

Dazu zählen unter anderem der Ausbau der elektronischen Patientenakte mit der erweiterten Berechtigungssteuerung durch den Versicherten in Stufe 2, die sukzessive Einführung des E-Rezeptes, die Einführung des E-Mail-Dienstes KIM zur Kommunikation im Medizinwesen, die Einführung der eAU, sowie die Einführung der Möglichkeit die bereits angesprochenen digitalen Gesundheitsanwendungen zu verschreiben. Bedingt durch diese fortschreitende Digitalisierung haben sich umfangreiche Erweiterungen und Änderungen für die Praxisverwaltungssysteme und die Komponenten der dezentralen Telematikinfrastruktur in den Praxen ergeben, um der umfangreichen Änderung der Anforderungen an die IT-Sicherheit gerecht zu werden. Die Zuständigkeiten des BSI wurden bereits in Kapitel 3.1 dargelegt.

Die zur Anbindung von Praxen und Krankenhäusern an die TI verwendeten Konnektoren werden jeweils nach Erreichen des Endes der Gültigkeitsdauer der erforderlichen Zertifikate ausgetauscht bzw. aktualisiert. Dies ist dem Umstand geschuldet, dass die Gültigkeit der Zertifikate grundsätzlich auf fünf Jahre beschränkt ist. Das BSI sieht weiterhin einen verantwortungsvollen Umgang mit ablaufenden Zertifikaten der Konnektoren als zwingendes Instrument zur Beibehaltung des für die Telematikinfrastruktur erforderlichen sehr hohen Sicherheitsniveaus. Weitergehend wurde in diesem Jahr medienwirksam von

verschiedenen Maßnahmen der Analyse und des Reverse-Engineerings von Konnektoren in Verbindung mit deren integrierten gSMC-K (gerätespezifische Secure Modul Card des Konnektors) berichtet, welche sich auf die Sicherheit der Konnektoren und die Notwendigkeit des derzeit gestarteten Konnektoraustauschs nach Zertifikatsablauf fokussierten. Die dargestellte Untersuchung und die Modifikationen setzten dabei voraus, dass gegen Annahmen an die geschützte Betriebsumgebung verstoßen wird und ein ungehinderter direkter Zugriff über einen großen Zeitraum auf den Konnektor möglich ist. In Hinblick auf die Optionen des Umgangs mit Konnektoren, deren Zertifikatablauf mittelfristig bevorsteht, wurde seitens der gematik in Abstimmung mit dem BSI bereits eine Alternativlösung spezifiziert.

Zusätzlich zu der IT-Sicherheit in den Arztpraxen, welche durch die Verwendung der von der gematik erarbeiteten Anwendungen (eAU, E-Rezept, e-PA, KIM, etc.) Einzug hält, definiert § 75b SGB V die Zuständigkeit der Kassenärztlichen Bundesvereinigung (KBV) und Kassenzahnärztlichen Bundesvereinigung (KZBV). Diese veröffentlichen im Einvernehmen mit dem BSI IT-Sicherheitsrichtlinien [10] [11]. Bestimmte Basis-Anforderungen gelten für alle Praxen, abhängig von der Praxisgröße gelten zusätzliche Anforderungen. Fast alle Anforderungen der in 2021 in Kraft gesetzten IT-Sicherheitsrichtlinien sind mittlerweile wirksam geworden, so dass sie von den Praxen erfüllt werden müssen. Die KBV und KZBV erarbeiten gemeinsam mit dem BSI Aktualisierungen der IT-Sicherheitsrichtlinie, sodass diese dem Stand der Technik entspricht. Darüber hinaus veröffentlicht das BSI Hinweise für die Leistungserbringer bzw. Praxisbetreibende, sodass die Steigerung der IT-Sicherheit in den Praxen voranschreiten kann [12].

3.5 Kritische Infrastrukturen

Die Auswertung vergangener Vorfallsmeldungen aus dem KRITIS-Sektor Medizinische Versorgung zeigen eine hohe Bereitschaft der Betreiber, ihre Vorfälle an das BSI zu melden. Dies ist sehr hilfreich, um ein Gesamtlagebild für den KRITIS-Bereich zu erstellen und um sanitarisierte Warn- oder Informationsmeldungen an registrierte Betreiber zielgruppenorientiert zu versenden. Die Sanitarisierung beschreibt das Entfernen von schutzbedürftigen Informationen aus einer Meldung, während relevante Informationen bestehen bleiben. Fast die Hälfte der eingegangenen Meldungen aus der Medizinischen Versorgung im Jahre 2022 bezogen sich auf einen Ausfall oder eine Beeinträchtigung der kritischen Dienstleistung im Sektor. Als Grund dafür wurde größtenteils technisches Versagen angegeben. Im Bezug zu den Prüfungen nach § 8a lässt sich feststellen, dass die meisten Mängel ebenfalls aus dem Bereich „Technische Informationssicherheit“ stammen, gefolgt von eher organisatorischen Mängeln im Hinblick auf die Etablierung und den Betrieb des Management-Systems für Informationssicherheit (ISMS). Seitens Labor- und Pharmabetreibern wurden 2021 und 2022 ca. 20 Meldungen abgegeben. Bei der Hälfte der Meldungen handelt es sich auch hier um technisches Versagen.

Insgesamt wurden im KRITIS-Bereich Gesundheit (Pharmazie, Labore und Medizinische Versorgung) bei einem Fünftel der Meldungen Angriffe angegeben. Bei diesen lässt sich ein Fokus auf die Dienstleister der Betreiber als Einfallstor feststellen. Anstatt Unternehmen und Behörden direkt anzugreifen, zielen die sogenannten Supply-Chain-Angriffe auf Anbieter, Lieferanten und die etablierten Lieferketten ab. Indem Produkte bereits bei den Herstellern oder Drittanbietern kompromittiert werden, beschränkt sich der mögliche Schaden nicht nur auf das angegriffene Unternehmen selbst, sondern weitet sich auf die in der Wertschöpfungskette nachgelagerten Unternehmen aus. Dieser Multiplikator macht Supply-Chain-Angriffe für Kriminelle besonders lukrativ und erklärt das vermehrte Auftreten solcher Attacken. Dies gilt nicht exklusiv für den Sektor Gesundheit, da sich diese Angriffe über Sektoren- und Ländergrenzen hinaus beobachten lassen.

4. Ausblick

Die Sicherheitslage im Netzwerk der Telmatikinfrastruktur wird regelmäßig überwacht und orientiert sich an strengen Spezifikationen. Die Sicherheitslage in den daran angeschlossenen Netzen, wie die der Arztpraxen, ist hingegen bisher kaum erfasst, obwohl sie essentiell für die Verarbeitung sensibler Gesundheitsdaten und der Patientensicherheit ist. Aus diesem Grund wurden durch das BSI neue Projekte gestartet, um die Sicherheitslage in Arztpraxen zu analysieren.

Das Projekt CyberPraxMed hat das Ziel, durch eine Umfrage den Netzwerkaufbau und die Ausstattung typischer Arztpraxen zu erfassen und die Sicherheitsrisiken einzuschätzen. Insbesondere soll eine Statistik die Frage beantworten, wie häufig sich der Konnektor im Parallelbetrieb zu einem privaten, konventionellen Router befindet und damit seine Schutzwirkung nicht vollständig entfalten kann. Darüber hinaus soll auch die IT-Kompetenz des Personals, des Arztes und eines gegebenfalls beauftragten IT-Dienstleisters bestimmt werden. Zusätzlich sollen Korrelationen der IT-Sicherheit mit der Praxisgröße, des Praxistyps (Hausarztpraxen, Zahnarztpraxen und Psychotherapie-Praxen) und der geographischen Lage (ländliche Regionen und Städte) untersucht werden. Das Ziel des Projekts ist ein öffentlich verfügbarer Bericht, der die Sicherheitslage in den Praxen aufzeigt und für häufig erkannte Sicherheitsprobleme eine Liste mit empfohlenen Maßnahmen vorlegt, sodass Ärzte mit möglichst geringem Aufwand eine möglichst hohe Sicherheit erreichen können. Der Bericht soll zudem auch für Menschen mit wenig IT-Kompetenz verständlich sein. Ergänzt wird diese Aktivität durch eine Sicherheitsuntersuchung von Praxisverwaltungssystemen (PVS). Ein PVS gehört zur Grundausstattung für das Praxismanagement von Leistungserbringern. Es wird zur Organisation und Dokumentation der Praxisaufgaben verwendet und bietet den oben genannten Leistungserbringern die Nutzung von bereits erwähnten Anwendungen aus der Telematikinfrastruktur. Hierunter fallen insbesondere Softwarelösungen für die Verwaltung von Patientendaten, Dokumentation von Arztgesprächen, Befunden und Medikationen, ein Terminplanungssystem, die Abrechnung ärztlicher Leistungen und eine Kommunikationsplattform zum fachlichen Austausch zwischen Leistungserbringern. Durch die zentrale Rolle eines PVS innerhalb der Arbeitsprozesse von Leistungserbringern, kommt dem PVS eine besondere Rolle zu. Die Software wird ständig weiterentwickelt und muss bei den Leistungserbringern aktualisiert werden, um mit der Telematikinfrastruktur reibungslos zusammenzuwirken und neue Anwendungen unterstützen zu können. Aus diesem Grund sollen im Rahmen des Projektes „Sicherheit von Praxisverwaltungssoftware“ (SiPra) einige PVS auf deren IT-Sicherheit geprüft und die Erkenntnisse den Anwenderinnen und Anwendern zur Verfügung gestellt werden, damit diese Konfigurationen bei ihren eigenen Systemen vornehmen können. Zusätzlich zu der Möglichkeit, die Ergebnisse unmittelbar zur Verbesserung der IT-Sicherheit in verwendeten Systemen zu nutzen, können die Ergebnisse als Grundlage möglicher industrieller Verbesserungen dienen, sodass ggf. Industriestandards etabliert werden können.

Literatur-verzeichnis

[1] https://www.bundesgesundheitsministerium.de/e-health-initiative.html, November 2022

[2] https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health.html, November 2022

[3] https://diga.bfarm.de/, Dezember 2022

[4] https://www.gesetze-im-internet.de/bsig_2009/__2.html, Oktober 2022

[5] https://www.gesetze-im-internet.de/bsi-kritisv/anhang_5.html, Oktober 2022

[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/ManiMed_Abschlussbericht.html, November 2011

[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/eCare_Abschlussbericht.html, November 2022

[8] https://www.golem.de/news/gesundheitsapp-trotz-zulassung-sicherheitsluecken-in-app-auf-rezept-2010-151471.html, Oktober 2022

[9] https://zerforschung.org/posts/datenabfluss-auf-rezept/, November 2022

[10] https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf, Oktober 2022

[11] https://www.kzbv.de/it-sicherheitsrichtlinie-75b-kzbv-v1-01-0121.download.e97ec0837147f4639f-3b4c32e5775c84.pdf, November 2022

[12] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/E-Health/Hinweise-IT-Sicherheitsrichtlinie-SGB/Hinweise_IT-Sicherheitsrichtlinie-SGB.html, Oktober 2022

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0

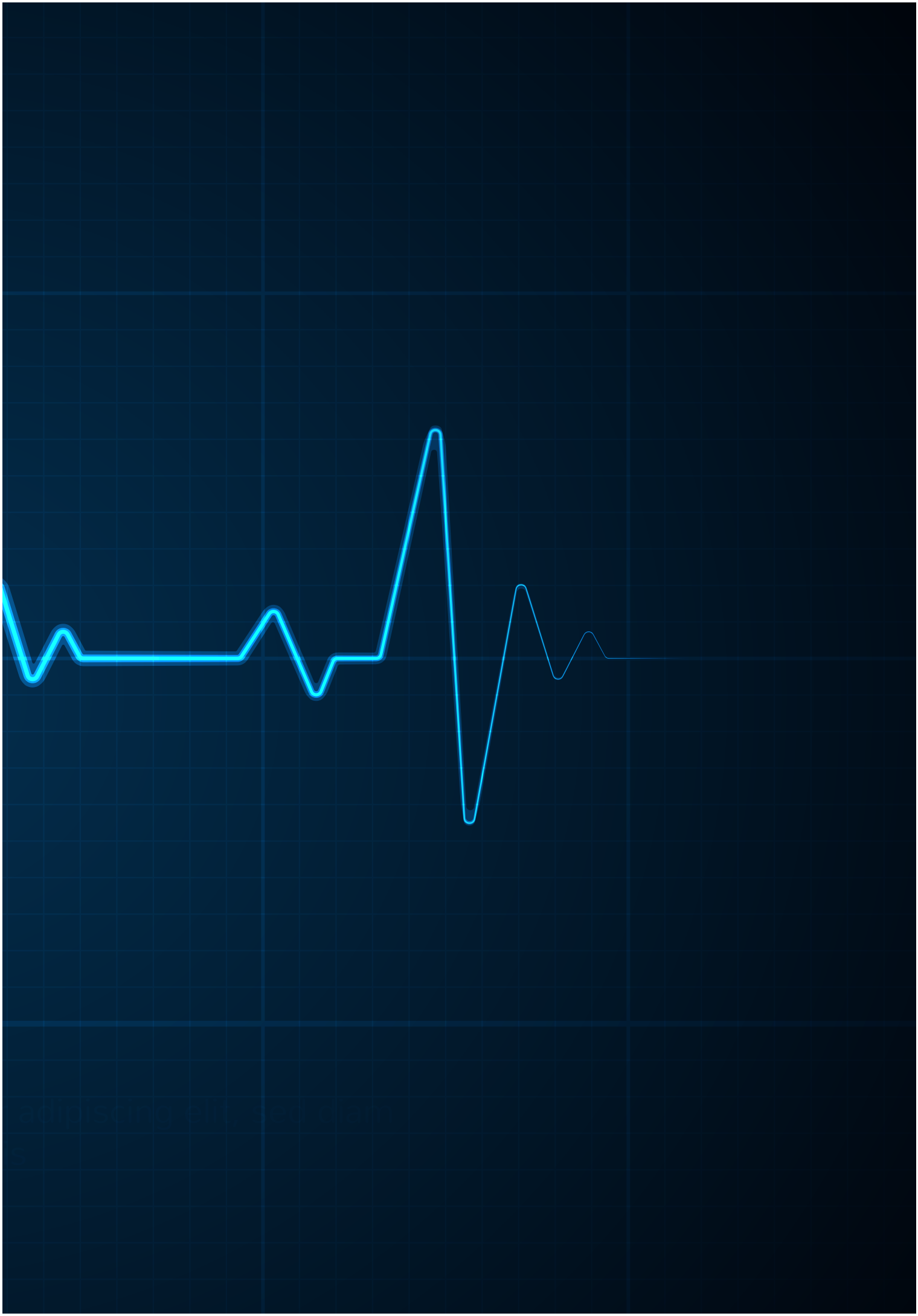
Kontakt
referat-di24@bsi.bund.de

Stand
Dezember 2022

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 © anttoniart, S. 2 und S. 35: AdobeStock © natrot, S. 4/5: AdobeStock © Gorodenkoff, S. 6/7: AdobeStock © Monet, S. 8: AdobeStock © ipopba, S. 11: AdobeStock © sitthiphong, S. 12: AdobeStock © Soeren, S. 16: AdobeStock © Prostock-studio1, S. 20: AdobeStock © StratfordProductions, S. 22: AdobeStock © Vadim Pastuh, S. 25: AdobeStock © likoper, S. 26: AdobeStock © Maksym Povozniuk, S. 30: AdobeStock © Gorodenkoff



Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582- 0
E-Mail: bsi@bsi.bund.de
www.bsi.bund.de