Cloud-Infrastrukturen für ein sicheres Gesundheitswesen

TELEMATIK-INFRASTRUKTUR 2.0

Damit die medizinische Versorgung weiterhin flächendeckend gewährleistet werden kann und den explodierenden Kosten Einhalt geboten wird, muss ein Gesundheitswesen der Zukunft auf digitalen Technologien basieren. Die Kritikalität der entsprechenden Health-Services ruft IT-Sicherheit auf den Plan – die Sensibilität der im Gesundheitswesen verarbeiteten Daten den Datenschutz. Ein zukunftsfähiges Gesundheitswesen braucht einen stringenten Rechtsrahmen, eine moderne cloudbasierte Telematikinfrastruktur, die je nach Sicherheitsbedarf in verschiedenen Modellen umgesetzt werden kann, einen restriktiven Umgang mit globalen Public-Cloud-Providern, eine besonders gesicherte, leistungsstarke Forschungsdateninfrastruktur – etwa zur Optimierung von KI-Fähigkeiten, sichere Gesundheitsanwendungen und einiges mehr. Hier ein Ausblick.

Der demografische Wandel ist für viele Länder eine zentrale Herausforderung des 21. Jahrhunderts. Gerade in den jeweiligen Gesundheitssektoren fehlen mehr und mehr akademische und medizinisch-helfende Fachkräfte in mehreren Teilbereichen des Gesundheitssektors. Durch die gestiegene Lebenserwartung und eine dadurch einhergehende stetig alternde Bevölkerung steigen die Kosten im Gesundheitswesen von Jahr zu Jahr rasant an.

Ein modernes, digitales Gesundheitswesen schafft kostensparende Vorsorge-, Diagnostik- und Behandlungsmöglichkeiten. Darüber hinaus erleichtert es die Kommunikation zwischen den Akteuren erheblich. Mittels Gesundheitsapplikationen kann die Gesundheitsversorgung jedes Einzelnen besser gesteuert werden. Telemedizin erlaubt eine direkte medizinische Versorgung der Patienten, egal wo diese sich gerade aufhalten. Maschinelles Lernen als Teilbereich der künstlichen Intelligenz erschließt künftig Zusammenhänge auf Basis von unstrukturierten Beispieldaten zu Forschungszwecken und zur Analyse. Dies ermöglicht, etwaige Krankheiten oder Vorfälle wie Diabetes, Adipositas, Schlaganfall, Krebs und vieles mehr im Vorfeld zu identifizieren. Überdies kann künstliche Intelligenz auch die Versorgung der Patienten nachhaltig verbessern.

Um diese Ziele erreichen zu können, müssen Forschungsdatenbanken, welche die benötigte Menge an Daten sammeln, in die Cloud-

Infrastruktur eingebunden werden. Denkbar sind auch telemedizinische Netzwerke zur unmittelbaren Notfallversorgung in Echtzeit, beispielsweise bei einem Schlaganfall. Wearables, die Vitalfunktionen zur Lebenserhaltung oder Fernüberwachung beziehungsweise -Steuerung augenblicklich zu übermitteln, wären Teil dieser Infrastruktur. Möglich ist ein automatischer Informationsaustausch zwischen Maschine und Rechenzentrum oder eine Kommunikation der Endgeräte mit einer zentralen Leitstelle als Kontrollinstanz. Gesundheitsapplikationen zur Abrechnung, zur Gesundheitsvorsorge, als elektronisches Rezept oder als Dashboard zum Informationserhalt sind in diesem Gesundheitsnetzwerk im Hinblick auf seine Wirtschaftlichkeit unabdingbar.

EIN STRINGENTER RECHTSRAHMEN ALS GRUNDLAGE

Die Bewahrung der Datenschutzziele ruft einen Rechtsrahmen auf den Plan, der alle Teilbereiche der Cloud-Infrastruktur abdeckt und damit für die Digitalisierung verbindliche Mindestanforderungen und Meldepflichten in der kritischen Infrastruktur festlegt. Zugleich muss der Rechtsrahmen auch die höchstmögliche Verfügbarkeit der digitalen Health-Services fördern. Die Voraussetzungen für die Umsetzung dieser Anforderungen gelten in Deutschland und in der Europäischen Union als vorbildlich. In Deutschland beispielsweise legt das IT-Sicherheitsgesetz einen Standard für die kritische Infrastruktur (KRITIS) fest, zu der neben Energie, Transport, Wasser und Telekommunikation auch der Gesundheitssektor gehört. Dieser Mindeststandard schreibt zum Beispiel den Einsatz von Komponenten zur Angriffs- und Anomalieerkennung, die Nutzung sicherer Protokolle zur Datenübertragung und vieles mehr vor.

Darüber hinaus unterliegen Sicherheitsvorfälle einer Meldepflicht, die bei Unterlassung erhebliche Geldbußen nach sich ziehen. Analog dazu erfolgten Rechtsänderungen im Telekommunikations- und Telemediengesetz zur Steigerung der Informationssicherheit im Internet. Die Verarbeitung personenbezogener Daten wird innerhalb der Europäischen Union länderübergreifend in der Europäischen Datenschutz-Grundverordnung (EU-DS-GVO) und für nationale Regelungen im Bundesdatenschutzgesetz (BDSG) geregelt. Explizit für den Gesundheitssektor wurden weitere Gesetze erlassen. Dazu gehört das „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen" (E-Health-Gesetz), das strenge Anforderungen an den Aufbau der Infrastruktur des Gesundheitssektors vorschreibt und die Einführung von digitalen Gesundheitsanwendungen überwacht. Ein weiteres Gesetz ist die Digitale-Gesundheitsanwendungen-Verordnung (DiGAV), das digitale Anwendungen unter anderem auf die Einhaltung von Sicherheitsanforderungen prüft. Im Jahre 2021 wurde es durch das Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) ergänzt. Es schreibt eine digitale Modernisierung der Versorgung und Pflege vor und überwacht den vorgeschriebenen gesetzlichen Datenschutz.

Damit die Interoperabilität im Gesundheitswesen gewährleistet wird, wurde die Gesundheits-IT-Interoperabilitäts-Governance-Verordnung (GIGV) ratifiziert. Dabei gibt es Überschneidungen mit weiteren Gesetzen, wie zum Beispiel dem Sozialgesetzbuch. Auf europäischer Ebene existiert zudem die europäische Medizinprodukte Verordnung (Medical Device Regulation (MDR)). Da sie innerhalb der Europäischen Union novelliert wurde, muss sie nicht in nationales Recht umgesetzt werden. Die Verordnung stellt Anforderungen an die Hersteller von Medizinprodukten, die der Qualität und Rückverfolgung der Medizinprodukte dienen. Dazu gehört unter anderem die MDR-konforme Dokumentation des User Interfaces, von Risikoanalysen und Produktspezifikationen. Darüber hinaus müssen Zertifikate vom Hersteller bereitgestellt werden. Künftig dürfen Gerätezulassungen in Europa nur erfolgen, wenn Konformität mit der Verordnung besteht.

Der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) des Bundesamtes für Sicherheit in der Informationstechnik (BSI), spezifiziert die Mindestanforderungen an den Betrieb der zentralen Komponente Cloud Computing.

Ein stringenter Rechtsrahmen mit wenigen übergeordneten Gesetzen und vielen juristischen Spezifikationen für die einzelnen Teilbereiche der Infrastruktur Gesundheitswesen ist somit übersichtlich, flächendeckend und dadurch absolut zielführend. Dadurch erleichtern sie Unternehmen den Einstieg in den jeweiligen Geschäftszweig. Die genannten Vorschriften und Gesetze in den USA sind beispielsweise kompakt in den Gesetzen HIPAA und HITECH verortet. Die Anforderungen an die IT-Sicherheit haben im Vergleich zu Deutschland denselben Sicherheitsstandard. Nach den Ergänzungen im HITECH ähnelt dieses Gesetz der EU-DS-GVO und ermöglicht einen umfassenden Datenschutz im amerikanischen Gesundheitssektor.

Ergänzend wurden von der Food and Drug Administration im Jahre 2022 ein aktualisierter Leitfaden zur Gewährleistung der Cybersicherheit von medizinischen Geräten verabschiedet. Ähnlich dem europäischen MDR müssen demnach Spezifikationen und Maßnahmen zur Cybersicherheit umgesetzt werden. Den Leitfaden gab es schon länger – wegen mehrerer Cybersicherheitsvorfälle in Krankenhausnetzwerken war jedoch eine Anpassung notwendig geworden. Da die gesamten Richtlinien und Bestimmungen für das Gesundheitswesen in den USA in nur wenigen Gesetzen geregelt sind, zeigen diese sich außerordentlich unübersichtlich. Aufgrund zahlreicher Überschneidungen wird der HIPAA zu einem schwer verständlichen und kaum zu überblickendem Gesetzeswerk.[1] Unternehmungen im amerikanischen Gesundheitssektor erfordern daher begleitend einen Rechtsbeistand, um Konformität zu erreichen.

DIE ZENTRALE KOMPONENTE: CLOUD COMPUTING

Die Cloud-Architektur kann je nach Sicherheitsbedarf in verschiedenen Bereitstellungsmodellen umgesetzt werden. Eines dieser Modelle ist die Public Cloud, die der Allgemeinheit zur Verfügung steht. Die Alternative dazu ist das Private-Cloud-Modell. Es steht nicht der Allgemeinheit zur Verfügung, sondern nur ausgewählten Benutzern innerhalb der entsprechenden Organisation. Die Cloud Services und die IT-Infrastruktur werden auf firmeneigenen Rechenzentren gehostet und befinden sich daher im eigenen Intranet. Zur Kostenreduktion kann das Hosting kann auch auf einen Dienstleister ausgelagert werden, der entsprechend abgeschottete Bereiche anbietet.

Die Hybrid Cloud kombiniert die beiden Bereitstellungskonzepte Public und Private Cloud. Hierbei sollen die Vorteile der jeweiligen Konzepte genutzt: Die Datenhaltung wird innerhalb des Unternehmensnetzwerkes organisiert, während über Webapplikationen der öffentlichen Cloud die Zugangsberechtigten weltweit und jederzeit Zugriff auf die Daten haben. Die Vorteile sind Kosteneffizienz, Skalierbarkeit und Flexibilität bei geringstmöglichem Datenrisiko.

Eine weitere Möglichkeit der Implementierung ist die Multi-Cloud-Architektur. Der Unterschied zur hybriden Cloud ist die Vielzahl an Cloud-Modellen gleichen Typs. Die Multi-Cloud löst zum Beispiel Abhängigkeiten von einzelnen Cloud-Anbietern auf. Auch die separate Nutzung verschiedener Infrastruktur-Modelle ist dadurch möglich: Während in einer Cloud Webapplikationen im Software-as-a-Service-(SaaS-)Modell entwickelt und getestet werden, können parallel in der anderen Cloud im Infrastruktur-as-a-Service-(IaaS-)Modell die Daten verarbeitet werden. Entstehende Arbeitslast kann aufgeteilt werden. Durch verteilte Backups wird einem möglichen Failover vorgebeugt, die räumliche Nähe zum Provider verbessert die Performance. Die Nachbarschaft zu regionalen Providern garantiert zudem die Anwendung der nationalen Rechtsprechung.

Eine Community Cloud ist ein Zusammenschluss, bei dem mehrere Organisationen einer bestimmten Branche sich die gleichen Rechenzentren, IT-Infrastruktur und dieselben Anwendungen teilen. Sie fassen ihre eigenen privaten Clouds zu einer Community-Cloud zusammen. Der Zutritt ist nur für Teilnehmer möglich. Es entsteht eine Interessengemeinschaft, die sich vertraut und den Datenschutz und die Sicherheit der privaten Cloud genießt. Die Möglichkeit, sie bei einem Cloud Service Provider zu realisieren, besteht ebenfalls. Dort kann sie von den teilnehmenden Organisationen selbst, oder von einem externen Managed-Service-Provider (MSP) betrieben werden. Durch die gemeinsame Nutzung der verschiedenen Infrastrukturen und Anwendungen kommt es zu einer effektiven Verwendung der Ressourcen. Dies führt zu einer allgemeinen Kostenreduzierung.

CLOUD SERVICE PROVIDER ALS VERMIETER FÜR DEN GESUNDHEITSSEKTOR

Die größten Public Cloud Service Provider (CSPs) wie zum Beispiel Amazon (AWS), Google oder Microsoft haben das finanzielle Potenzial des Gesundheitssektors bereits seit Längerem erkannt. AWS for Health, Google und Microsoft HealthCare bieten Dienste wie die elektronische Patientenakte für Kunden an, die dort ihre gesamten Gesundheitsdaten speichern können. Je nach Kundenwunsch kann sie für Ärzte, Krankenhäuser etc. freigegeben werden. Darüber hinaus stehen Dienste für Telemedizin, künstlicher Intelligenz zur Diagnoseunterstützung und Dashboards zur Betriebsverwaltung und vieles mehr bereit. Diese bereits vorhandenen Cloud-Infrastrukturen zu nutzen, birgt aber erhebliche Gefahren. Vor allem bei der Nutzung der Dienste würde sich ein Gesundheitswesen zu stark von einem Provider abhängig machen. Häufig nutzen die einzelnen Provider proprietäre Formate und Schnittstellen, die nicht kompatibel mit anderen Anbietern sind. Dies führt dazu, dass die Portabilität einer Infrastruktur auf eine andere Plattform nicht ohne erhebliche Portierungs- und Integrationsprobleme möglich ist – wenn überhaupt. Die Folge wäre eine nicht akzeptable Abhängigkeit von einem einzigen Anbieter (Vendor-Lock-in Effekt).

Weiterhin betreiben Drittanbieter von Providern ihre Rechenzentren meist außerhalb der Europäischen Union. Das Gleiche gilt auch für die Cloud Provider, deren zahlreiche Serverlandschaften in einem internationalen Umfeld angesiedelt sind. Datenschutz, Informationspflichten, Insolvenzrecht, Haftung oder Informationszugriff für Dritte bewertet die Judikative in verschiedenen Ländern anders. Die Mehrzahl der Serverlandschaften großer CSPs befindet sich beispielsweise in den USA. Nach der Europäischen Datenschutz-Grundverordnung (EU-DS-GVO), dürfen dorthin keine Personendaten übertragen werden. Der sogenannte Patriot Act aus dem Jahre 2001 erlaubt es US-Behörden, auf Rechenzentren amerikanischer Provider sowohl im In- als auch im Ausland zuzugreifen und alle Daten, auch die von europäischen Unternehmen und Personen, zu transferieren. Ein Abkommen zwischen der Europäischen Union und den USA vom Jahre 2016 wurde vier Jahre später im Schrems-II-Urteil vom Europäischen Gerichtshof wieder gekippt. Das EU-US Privacy Shield entsprach nicht dem geforderten Sicherheitsniveau der DS-GVO. Trotz der beschriebenen Unwägbarkeiten hat das Oberlandesgericht Karlsruhe am 7. September 2022 in einem Beschluss den Ausschluss von Tochterfirmen der US-Cloud-Anbieter bei Vergabeverfahren wieder aufgehoben. Bindende Zusagen der Provider, Daten ausschließlich in Deutschland zu verarbeiten, reichen dabei als Zusicherung aus. Als Begründung wurden die Vorschriften zur Ende-zu-Ende Verschlüsselung und Pseudonymisierung herangezogen.

Rule	Gesetz	Gegenstand
	HIPAA	
Security Rule	Part 160 und Part 164; Subparts A und C	Nationale Standards zum Schutz persönlicher elektronischer Gesundheitsdaten. Angemessene administrative, physische und technische Schutzmaßnahmen.
Privacy Rule	Part 160 und Part 164; Subparts A und E	Datenschutz
Enforcement Rule	Part 160; Subparts C, D und E	Durchsetzungsrechte und -pflichten der staatlichen Behörden
Breach Notification Rule	Part 164; § 164, 400 - 414	Meldepflichten bei Zwischenfällen
Administration Requirements Rule	Part 162; Subparts D,F und I	Standard Gesundheitskennung für Gesundheitsdienstleister Standard Arbeitgeberkennung Allgemeine Bestimmungen für Transaktionen
Omnibus Rule		Änderung des HIPAA als Teil des HITECH Acts im Jahre 2013. Die Omnibus-Regel macht auch Geschäftspartner von betroffenen Einrichtungen für Verstöße haftbar wie z.B. Cloud-Anbieter.
	HITECH	
Promotion of Health Information Technology	Subtitle A; Part 1	Verbesserung der Qualität, Sicherheit und Effizienz der Gesundheitsversorgung, wie z.B., die Nutzung einer elektronischen Patientenakte und E-Rezepten
Privacy	Subtitle D; Part 1	Verbesserte Datenschutzbestimmungen und Sicherheitsbestimmungen (ähnlich der DSGVO), Meldepflichten (u. a. Gesundheitsministerium, Medien)

Gesetzgebung im amerikanischen Gesundheitssektor (Quelle: ifis)

AUFBAU EINER FORSCHUNGSDATEN-INFRASTRUKTUR FÜR EIN ZUKUNFTSFÄHIGES GESUNDHEITSWESEN

Damit zukünftige Fragestellungen im medizinischen Bereich unter Zuhilfenahme der künstlichen Intelligenz schneller gelöst werden, ist

es unerlässlich, große Mengen an Anamnese-, Diagnose- und Prognosedaten zu sammeln. Auch die Sammlung genetischer Daten wird diskutiert. Diese Datenerhebungen können helfen, Krankheitsbilder und deren Ursache schneller zu erkennen. Aussagen über den Krankheitsverlauf oder mögliche Folgeerkrankungen könnten frühzeitig getroffen werden. Behandlungen, die aufwendig und dadurch kostspielig sind, könnten bei jedem Patienten individuell und schneller angepasst werden. Mit zunehmender Kenntnis über individuelle Unterschiede der Patienten könnten gezielte und effektive Therapien frühzeitig und unter Vermeidung belastender Nebenwirkungen angewendet werden.

Damit in Zukunft in Deutschland eine zentrale Wissensbank mit Datenbeständen zur Verfügung steht, gründeten sich vier Konsortien, die im Rahmen der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung gefördert werden. Die Konsortien sind ein Verbund von Forschungseinrichtungen, Hochschulen, Unternehmen und Krankenhäusern mit dem Auftrag, Forschungs- und Patientendaten zu sammeln. Diese werden in Datenintegrationszentren zentral am jeweiligen Sitz verarbeitet und untereinander ausgetauscht.

Im wissenschaftlichen Kontext regelt die DS-GVO den Umgang mit diesen sensiblen Gesundheitsdaten. Darüber hinaus gestattet das EU-Unionsrecht den Nationalstaaten im Hinblick auf die Verarbeitung von wissenschaftlichen, historischen oder statistischen Forschungszwecken eigene Rechtsprechungen. Beispielsweise erlaubt es die Verarbeitung von Daten zu Forschungszwecken, wenn dies im öffentlichen Interesse liegt. Der Passus der zweckgebundenen Verarbeitung ist nicht immer möglich, da Forschungsziele gerade im medizinischen Bereich oft nicht von Anbeginn festgelegt werden können. Eine erweiterte Formulierung des Zwecks ist zwar möglich, bedarf aber einer Einwilligung der Betroffenen. Ebenso wird das Gebot der Datenminimierung konterkariert, da Forschungsvorhaben im Bereich KI und ML auf umfangreiche Forschungsdaten angewiesen sind. Zudem unterliegen sie nicht dem Recht auf Vergessen. Dieses Sonderrecht ermöglicht es, diese Daten über das Forschungsvorhaben hinaus und auf unbestimmte Zeit zu speichern. Obwohl die DS-GVO und das BDSG Forschungsvorhaben an vielen Stellen privilegieren, verpflichten sie die Datenverarbeiter auch zu geeigneten Garantien für die betroffenen Personen. Dazu gehören vor allem technische und organisatorische Maßnahmen (TOM). Hierzu zählt die Zugangs-, Zugriffs-, Trennungs-, Verfügbarkeits- und Weiterverarbeitungskontrolle. Weitere Kriterien sind das Gebot der Pseudonymisierung und Anonymisierung, ein Reaktionsplan bei Sicherheitsverletzungen sowie datenschutzfreundliche Voreinstellungen, die das Widerrufsrecht für die Verarbeitung personenbezogener Daten vereinfachen.[2]

SICHERE GESUNDHEITSANWENDUNGEN ALS TEIL DER CLOUD-INFRASTRUKTUR

Wesentlicher Bestandteil eines modernen digitalen Gesundheitswesen sind entsprechende Anwendungen. Gerade mobile Anwendungen tragen dazu bei, die Bereiche Vorbeugung, Diagnose, Überwachung und Therapie entscheidend voranzubringen. Auch innerhalb der Verwaltung können mobile Anwendungen die Abläufe erheblich vereinfachen. Diese Aspekte tragen dazu bei, dass der gesamte Gesundheitssektor effizienter und kostensparender operieren kann. Die Problematik ist jedoch, dass die Anwendungen in wichtigen Geschäftsprozessen in der kritischen Cloud-Infrastruktur des Gesundheitswesens implementiert werden. Eine Vielzahl von Angriffsvektoren zielt direkt auf Sicherheitslücken in den Anwendungen, um sich Zugang zu Daten und Systemen zu verschaffen. Mittlerweile gelten sie als die größten Bedrohungen gegen IT-Systeme. Von Vorteil ist es daher, wenn die Entwicklung und das Testverfahren bereits in geschlossenen Containern innerhalb der Cloud abläuft. Dadurch verlässt die Software bis zur Veröffentlichung nicht das sichere Umfeld der Cloud.

Die einfache und schnelle Bereitstellung von Apps im Cloud-Umfeld hat dazu geführt, dass überwiegend Microservice-Architekturen umgesetzt werden. Der Vorteil der Microservices ist ihre Isolierung gegenüber anderen Services und die Verwendung unterschiedlicher Technologien, Programmiersprachen und Datenbanken. Der gesamte Softwarecode, der übersichtlich und klein gehalten wird, ist vor unerwünschten Zugriffspfaden durch zeilenweise Inspektion der Software geschützt. Durch die Separierung in verschiedenen Container wird die Anwendung zudem ausfallsicher. Darüber hinaus wurde ein Designansatz im IT-Umfeld entwickelt, der die Sicherheit der Software über den kompletten Lebenszyklus betrachtet: „Security by Design" reicht dabei von der Phase der Ideenfindung bis zum Lebensende einer Software. Der Vorteil hier ist ein deutlich reduziertes Risiko für Schwachstellen in der Anwendungssoftware.

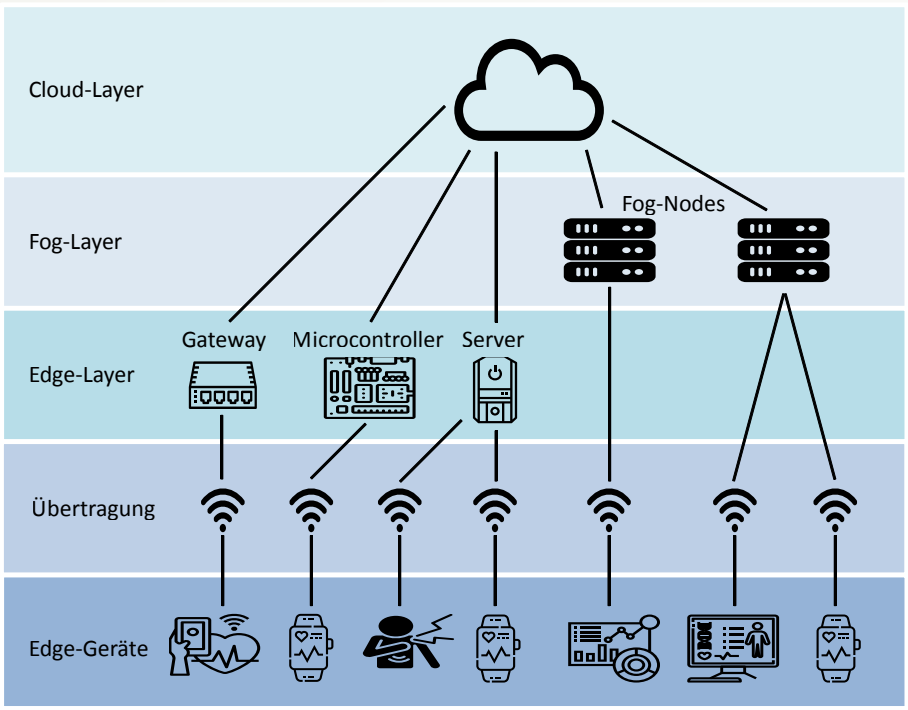
Die Transparenz aller unternommenen Schritte senkt auch die Wahrscheinlichkeit, Opfer eines Angriffs zu werden. Im Lebenszyklus einer Anwendung können verschiedene Prozesse und Maßnahmen zur Software-Sicherheit getroffen werden. Zu Beginn sollten alle betroffenen Gesetze und Richtlinien für Anwendungen im Gesundheitswesen zum Schutz der Informationssicherheit betrachtet werden. Ein wichtiges und verpflichtendes Werkzeug in Deutschland sind beispielsweise die Sicherheitskonzepte nach dem IT-Grundschutz. Von der O-WASP Foundation wird das Software Assurance Maturity Model (SAMM) zur Verfügung gestellt. Es ist ein Softwaresicherheitsmodell, das eine effektive und messbare Möglichkeit bietet, die Sicherheitslage rund um die Anwendung zu analysieren und zu verbessern. Dieses Modell wurde im Auftrag der Gematik bei einer 360-Grad-Sicherheitsanalyse genutzt, um verschiedene Dienste der Telematikinfrastruktur zu bewerten. Weitere Maßnahmen sind die Anwendung von Design-Prinzipien, Programmiermuster, die Durchführung einer Bedrohungsanalyse und vieles mehr. Das Security-by-Design-Konzept ist ein kontinuierlicher Prozess und endet erst mit dem End-of-Life einer Anwendung und der damit verbundenen Außerbetriebnahme.[3]

DEZENTRALE DATENVERARBEITUNG AM RANDE DER CLOUD-INFRASTRUKTUR

In einer künftigen IT-Infrastruktur im Gesundheitswesen könnte es zwingend nötig sein, dass Daten in Echtzeit verarbeitet werden müssen. Das gilt zum Beispiel für Wearables, die Vitalfunktionen erfassen und zur Lebenserhaltung oder Fernüberwachung beziehungsweise -steuerung auswerten. Um diese Herausforderung zu meistern, besteht die Möglichkeit, die Rechenleistung an den Rand des Netzwerkes zu verlagern, möglichst nahe an den Ort, wo die Daten erhoben werden. Mittels Mikrocontrollern am Endgerät oder kleinen Rechenzentren vor Ort findet die Datenverarbeitung statt.

Ein weiteres Modell ist der Aufbau eines Rechenzentrums in unmittelbarer Nähe zu den Edge-Geräten. Diese Rechenzentren verarbeiten meistens die Daten mehrerer Sensoren aus

einer Region. Diese beiden Modelle nennen sich Edge- und Fog-Computing. Entfernen sich die Serverlandschaften von der Kern-IT, etabliert sich eine Zwischenebene zwischen dem physischen Gerät und der zentralen Cloud. Dadurch wird die Kern-IT besser isoliert und ist weniger von Cyberangriffen bedroht. Das Verbleiben der Daten auf dem Endgerät erleichtert zudem, Compliance-Regelungen zu erfüllen. Kleinere Standorte verarbeiten weitaus weniger Daten als eine Hauptniederlassung, benötigen jedoch die gleichen Sicherheitsmaßnahmen. Zu den Kosten für die Informationssicherheit und die physische Sicherheit kommt auch der höhere Wartungs- und Administrationsaufwand hinzu. Weiterhin entstehen durch viele Endgeräte am Rand des Netzes weitere Angriffspunkte in der IT-Infrastruktur.

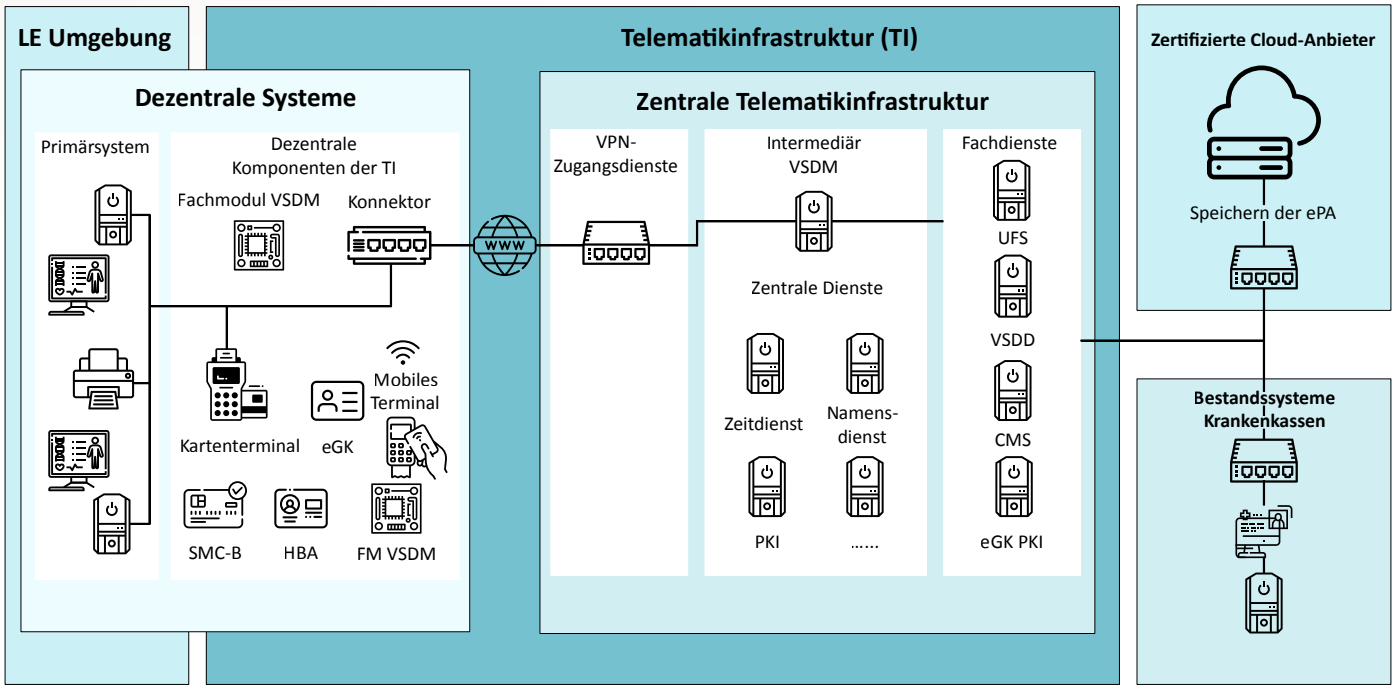


Darstellung der Verarbeitung von Daten am Rand der IT-Infrastruktur (Quelle ifis)

Künftig könnte zur Übertragung zu den jeweiligen Layern der Mobilfunk Standard 5G genutzt werden, der ein Network Slicing ermöglicht. Über einen Funkmast stehen diverse Netzwerke zur Verfügung, die einen Netzwerkausfall verhindern. Einige Netze sind für eine große Bandbreite und optimierte Latenz ausgelegt, andere wiederum unterstützen sicherheitskritische Übertragungen mit zusätzlicher Verschlüsselung. Diese Möglichkeit schafft nicht nur eine Auswahl für die jeweiligen Anforderungen, sondern auch Netzredundanz. Der Standard zur Verschlüsselung der Kommunikation ist im 5G-Netz das TLS-1.3-Protokoll. Dadurch werden Integrität und Vertraulichkeit der Daten geschützt. Darüber hinaus unterstützt 5G auch VPN. Software und Router sind für diese Technologie bereits verfügbar. Im 5G-Netz wird zudem die Teilnehmernummer – International Mobile Subscriber Identity (IMSI) – verschlüsselt übertragen. Dadurch bleiben Gesundheitsdaten völlig anonym und der Datenschutz entsprechend gewährleistet.[4]

DIE UMSETZUNG VON CLOUD-INFRASTRUKTUREN IM DEUTSCHEN GESUNDHEITSWESEN

Die Gematik GmbH ist die Dachorganisation der Telematikinfrastruktur (TI). Sie soll übergreifende IT-Standards für den Aufbau und den Betrieb einer IT-Infrastruktur im Gesundheitswesen entwickeln. Das Bundesministerium für



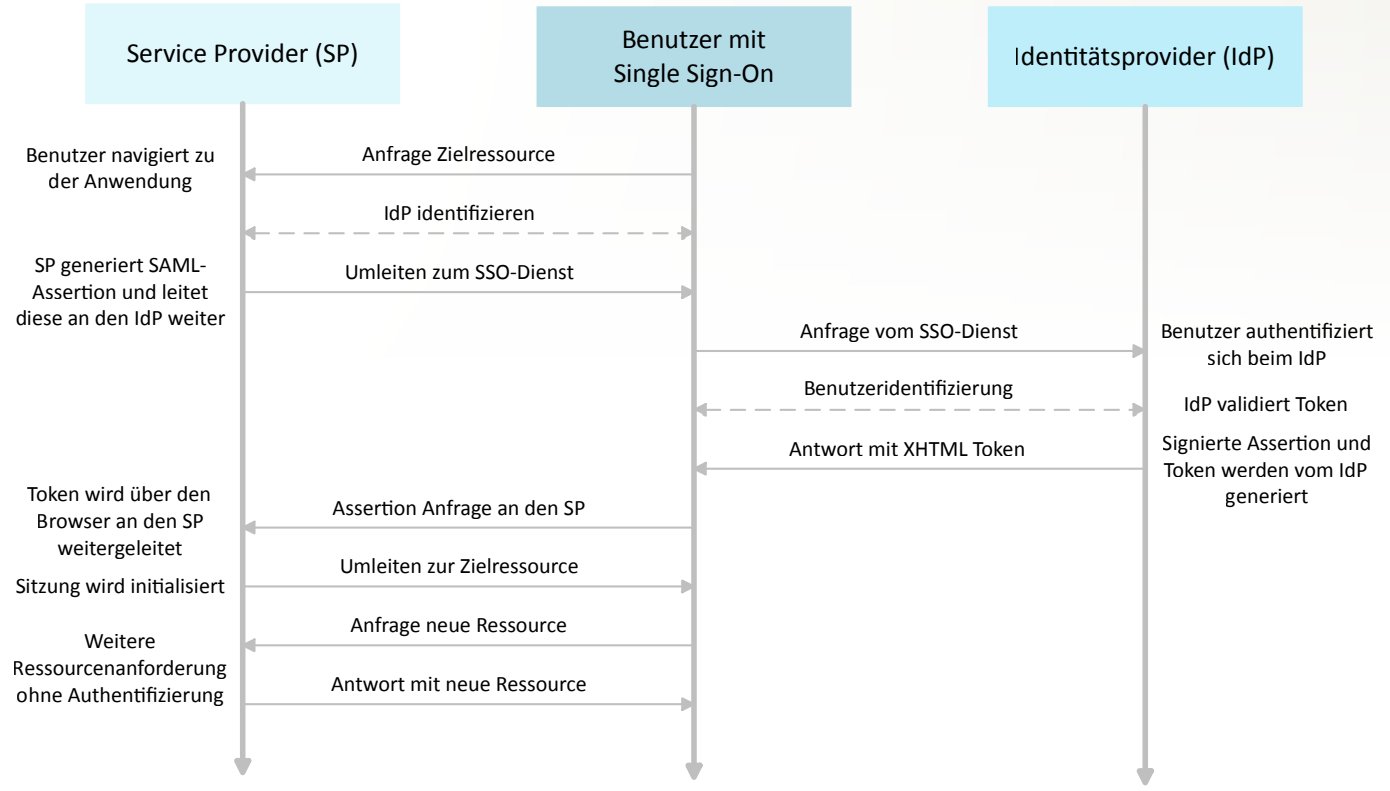
Darstellung der Telematikinfrastruktur (Quelle: ifis)

Gesundheit hält seit einer Gesetzesänderung im Jahre 2019 51 Prozent der Anteile. Auf Basis des Sozialgesetzbuchs wurde die Gematik verpflichtet, technische und organisatorische Verfahren zu erarbeiten. Sie steuert außerdem den Betrieb der Telematikinfrastruktur, Test und Zulassung der Dienste und Komponenten und reguliert die technischen Spezifikationen der erforderlichen Hardware, Software und Datenformate. Dazu wurde der zentrale Verzeichnisdienst Vesta verwirklicht, der die technischen und semantischen Standards gewährleistet. Die Interoperabilität zwischen den Komponenten und Anwendungen bleibt dadurch erhalten. Die verschiedenen Berechtigungskarten enthalten digitale Schlüssel und Zertifikate sowie die persönlichen Daten. Der digitale Schlüssel ist dabei die digitale Identität des Versicherten in der TI. Die Zertifikate ermöglichen dem Inhaber den Zutritt zur Telematikinfrastruktur.

Der Trust Service Provider (TSP) X.509-nonQES gehört zur Public-Key-Infrastruktur der Telematik und erstellt die Zertifikate für die Leistungserbringer zur Authentisierung. Darüber hinaus validiert er diese und führt eine Sperrliste für Zertifikate (Certificate Revocation List, CRL), deren Schlüsselmaterial kompromittiert wurde, deren Zertifikatsdaten ungültig sind oder die beim Verlassen der PKI-Organisation erloschen sind. Der TI-Konnektor ist das zentrale Gerät für den sicheren Zugang in das Netz der TI. Die gesamten Komponenten sind hinsichtlich ihrer IT-Sicherheit zuvor vom BSI geprüft und zertifiziert worden. Der Konnektor arbeitet ähnlich einem Router auf einem sehr hohen Sicherheitsniveau. Er baut ein virtuelles privates Netzwerk (VPN) zur TI auf. Für alle Ereignisse, die vom Konnektor an das Primärsystem gesendet werden, nutzt er das eigene Protokoll CETP (Connector Event Transport Protocol). Dieses leichtgewichtige, proprietäre Protokoll verlangt ein Abonnieren bestimmter Ereignistypen durch das Primärsystem. So können beispielsweise Ereignisse gezielt abonniert werden, sodass nur einzelne Arbeitsplätze die Informationen erhalten. Dies erhöht den Datenschutz innerhalb der Arztpraxis enorm.

Das Fachmodul VSDM-Konnektor baut beispielsweise eine Verbindung zum Versichertenstammdatenverzeichnis der Telematikinfrastruktur auf. Das E-Health-Modul ermöglicht das Speichern und Auslesen des Notfall- und Medikationsplans. Darüber hinaus wird das elektronische Senden und Empfangen der Arztbriefe ermöglicht. Eine zusätzliche Software kann auf dem Konnektor aufgespielt werden. Weiterhin ist eine Anbindung über den Konnektor an das sichere Netz der Krankenversicherer (SNK) gewährleistet. Das SNK ist in die TI mit eingebunden und ermöglicht den Krankenkassen in den Fachdiensten Update Flag Service (UFS), Kartenmanagementsystem (CMS) und Versichertenstammdatendienst (VSDD), die Daten zu aktualisieren. Beispielsweise können die Abrechnungen über das SNK online eingereicht werden.

Das bestehende Konzept wurde bereits zu Beginn der 2000er-Jahre entwickelt. Das derzeitige Konzept basiert auf Überlegungen und Voraussetzungen der damaligen Zeit. Die gesamte Technologie hat sich mittlerweile in Richtung Mobilität entwickelt, sodass der momentane Status eines abgeschotteten Netzes mit einem Zugang über Konnektoren nicht mehr zeitgemäß ist. Datensilos, die nur für wenige Bereiche zugreifbar sind, sollen aufgelöst und mobile Patientenversorgung möglich gemacht werden. Gesundheitsanwendungen sollen dabei befähigt werden, untereinander und mit den Nutzern frei zu kommunizieren. Darüber hinaus können Videosprechstunden künftig auch per Smartphone erfolgen.



Workflow zwischen Service Provider und Identitätsprovider mit Single Sign-on (Quelle: ifis)

Besonders für Mitarbeitende aus der Pflege sind mobile Einsatzszenarien eine mögliche effektive Alternative. Patienten können dann auch mobil auf die TI zugreifen. Mobile Messgeräte speisen ihre Daten unmittelbar in die neue TI 2.0 ein und sind dadurch schneller verfügbar. Dieses neue Konzept soll bis 2025 umgesetzt werden. Die bisherige Organisation entspricht der Umsetzung einer Community-Cloud, bei der alle Krankenversicherer bei verschiedenen internationalen Providern eigene private Clouds abonniert haben. Einer dieser Provider ist IBM Deutschland. Aufgrund des beschriebenen Drittstaatenproblems ist IBM Deutschland die fragmentierte Datenhaltung außerhalb Deutschlands untersagt und das Verbot in den Service Level Agreements dokumentiert. Bei Verstößen drohen den zertifizierten Providern nicht nur SLA-Strafgebühren, aus der DS-GVO resultieren zudem zusätzliche, sehr erhebliche Geldbußen. IBM musste sich zudem einem komplexen Zertifizierungsprozess der Gematik unterziehen.

Die Gewährleistung der Sicherheit und des Datenschutzes wird anstelle eines geschlossenen Netzes künftig durch einen Identitätsprovider (IdP) ersetzt. Dieser schränkt den Zugang auf die berechtigten Nutzer ein. Ein Identitätsprovider ist ein Dienst, der in einer Cloud gehostet wird und der mit einem Single Sign-on-(SSO-)Verfahren zusammenarbeiten kann. Die Kommunikation zwischen IdP und dem Service Provider erfolgt über Sicherheitsprotokolle, wie beispielsweise SAML, OpenID oder OAuth.[5] Der Prinzipal muss nicht zwangsläufig ein menschlicher Benutzer sein. Auch Geräte, wie zum Beispiel Wearables, könnten via ID oder anderer Faktoren angemeldet und damit Teil der Infrastruktur werden. Anstelle von Zertifikaten kann die neue TI 2.0 auf andere Identitätsverfahren umgestellt werden. Manche künftige Bereiche der Cloud-Infrastruktur könnten auf Ausfallsicherheit angewiesen sein. Da dies für Zertifikate nicht gilt, sind diese beispielsweise auch in Kernkraftwerken und Chemieanlagen verboten.

ZUSAMMENFASSUNG

Es hat sich gezeigt, dass ein Rechtsrahmen mit übergeordneten Gesetzen für eine kritische Infrastruktur und Gesetzen, die darüber hinaus alle Teilbereiche der IT-Infrastruktur abdecken, im Hinblick auf IT-Sicherheit und Datenschutz eine sehr vielversprechende Strategie ist. Am Rande des Gesundheitsnetzwerkes werden künftig große Mengen Daten zur Überwachung und Betreuung verarbeitet und zu statistischen Zwecken weitergeleitet. Der 5G-Standard bietet unter dem Gesichtspunkt Ausfallsicherheit, Bandbreite, Anonymität und Sicherheit hierfür eine geeignete Technologie. Eine Wissensdatenbank ist zentraler Bestandteil einer Infrastruktur Gesundheitswesen.

Mittels künstlicher Intelligenz und maschinellen Lernens können anhand großer Datenmengen künftig Krankheiten frühzeitig erkannt und behandelt werden. Für diese Forschungsdatenbank hat der Gesetzgeber in Deutschland den Umgang mit diesen Daten bereits gesetzlich bestimmt. Gesundheitsanwendungen müssen entlang des Security-by-Design-Konzepts begleitet werden. Da sie oftmals das Einfallstor für Angriffe sind, ist ihre sichere Entwicklung im Cloud-Umfeld unerlässlich. Lediglich die Cloud-Forensik, zum Aufspüren von Sicherheitsvorfällen und zum Sammeln sowie Aufbewahren der Datenspuren, konnte in den letzten Jahren nicht mit der voranschreitenden Cloud-Technologie mithalten. Dennoch wird auch sie in Zukunft entscheidende Schritte nach vorn machen. Allen voran das National Institute of Standards and Technology entwickelt Werkzeuge, welche digitale Spuren in der Cloud aufspüren und sammeln können.[6]

Eine durch Mobilität getriebene IT-Infrastruktur schraubt marginal die Sicherheit herab – durch den Verzicht auf ein geschlossenes Netzwerk mit wenigen Teilnehmern. Es sind jedoch alle Technologien vorhanden, damit auch diese moderne Telematikinfrastruktur 2.0 geschützt werden kann. Die beschriebene TI 2.0 könnte ein Vorreiter für eine einheitliche europaweite Implementierung eines Gesundheitswesens werden. Dafür spricht die konsequente Berücksichtigung aller Aspekte der Informationssicherheit unter Beachtung der Mobilitätskriterien. ■

Literatur

[1] *C. Johner: „HIPAA in Kurzform", Johner Institute, 2022*

[2] *M. Bäcker, S.Golla: „Handreichung Datenschutz", BMBF, 2020*

[3] *I. Wigmore: „Security by Design", TechTarget, 2022*

[4] *O. Schonschek – Mehr Bandbreite – mehr Datenschutz, Datenschutz Praxis, 2019*

[5] *N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigen-schaften von Cyber-Sicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2022*

[6] *N. Pohlmann, D. Schwarzkopf: „Blick in die großen „Verstecke" von Cyberkriminellen – Herausforderung für die digitale Forensik", IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2021*

DETLEF SCHWARZKOPF
studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Cyber-Sicherheit in Cloud-Infrastrukturen.

TOBIAS URBAN
ist Postdoktorand im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen und beschäftigt sich unter anderem mit der Sicherheit im Gesundheitswesen.

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.