
2.1 Bisherige Entwicklung des Marktes

Die Digitalisierung in verschiedenen Wirtschaftszweigen sowie in privaten und staatlichen Einrichtungen hat auch einen Markt für die elektronische Übertragung von Gesundheitsdaten geschaffen. Zu Beginn des Jahres 1995 wurde die erste elektronische Gesundheitskarte (eGK) von den Krankenkassen angeboten, welche eine schnellere und effizientere Kommunikation zwischen Patient und Arzt sowie Arzt und Krankenkasse ermöglichen sollte. Die eGK gilt als Berechtigungsnachweis zur Inanspruchnahme von Leistungen der Gesetzlichen Krankenkasse und löst seit 1. Januar 2015 die vorherige Krankenversicherungskarte (KVK) vollständig ab.¹

Auf der elektronischen Gesundheitskarte sind folgende Daten gespeichert:²

- Bezeichnung der ausstellenden Krankenkasse, einschließlich eines Kennzeichens für die Kassenärztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat
- Familienname und Vorname des Versicherten
- Geburtsdatum
- Geschlecht
- Anschrift
- Krankenversichertennummer
- Versichertenstatus, für Versichertengruppen nach SGB § 267 Abs. 2 Satz 4 in einer verschlüsselten Form, Tag des Beginns des Versicherungsschutzes
- bei befristeter Gültigkeit der Karte das Datum des Fristablaufs

¹BSI Gesundheitskarte.

²SGB Fünftes Buch, § 291.

Da Stammdaten auf der eGK nicht verändert werden können, ist bei einem Wechsel der Kundenanschrift stets eine neue Karte bei der entsprechenden Krankenkasse einzufordern. Nach Einführung der eGK entstanden diverse alternative Möglichkeiten Daten zu übermitteln, jedoch behielt die eGK bis heute ihre analoge Übertragungsart, durch Auslesen der Daten über ein definiertes Lesegerät.

Seit 1995 sind verschiedene Übertragungsprotokolle und Technologien erschienen und verschwunden. Die wenigen, die sich durchsetzen konnten und bis heute bestehen sind

- Bluetooth
- LAN (Local Area Network)
- HTTP (Hypertext Transfer Protocol)
- NFC/RFID (Near Field Communication/Radio-Frequency Identification)
- Prozessor-Chipkarten

Durch die zunehmende Vernetzung von Geräten hat sich die Internetnutzung vom stationären Internet zum mobilen Internet verschoben. Zudem hat sich durch den technischen Fortschritt von z. B. Bluetooth 1.0 zu Bluetooth 4.0 die Geschwindigkeit der Datenübertragung potenziert. Durch eine parallele Verbesserung der Lithium-Akkumulatoren und der Speicherkapazität mobiler Geräte ist die Nachfrage nach stationären internetfähigen Geräten in Form von Desktop-PCs stark zurückgegangen. Als abhörsicher oder sicher gegen unbefugtes Eindringen gelten Bluetooth-Übertragungen nur dann, wenn sie als Verbindung mit mehrstufiger dynamischer Schlüsselvergabe betrieben werden. Durch diese Verschiebung sind neue Märkte entstanden und neue Arten digitaler Informationsübertragungen haben sich entwickelt.

Die Near-Field-Communication-Technologie (NFC-Technologie) erlaubt es beispielsweise, Informationen in Reisepässen zu digitalisieren, Türen mit Smartphones zu öffnen, Haustiere zu identifizieren und Informationen an öffentlichen Orten über Tags (Beacons) verfügbar zu machen. Mit steigender Verbreitung von Smartphones und den damit verbundenen Möglichkeiten ist eine stetige Weiterentwicklung der Vernetzung zu erwarten.

Durch schnellere Kommunikationsmöglichkeiten und die fortschreitende Entwicklung der Transistoren sowie der Datenübertragung sind neben verschiedenen Infrastrukturen für die Krankenhaus-IT (auf diese wird in Kap. 6 genauer eingegangen) auch autarke Technologien entstanden, die die kontaktlose Übertragung von Daten durch Scannertechnologien und Induktionsspeicher ermöglichen. Als zum Ende der ersten Dekade des 21. Jahrhunderts mobile Endgeräte (Smartphones) und Apps erschienen, vermischten sich diese Technologien und mobile Endgeräte wurden zu universell einsetzbaren Geräten, die ab dem Jahr 2010 erste E-Health-Anwendungen in die Haushalte der Konsumente brachten.

Im Jahr 2014 kamen die ersten kommerziellen Smartwatches und Healthbands (smarte Armbänder) auf den Markt, die Statistiken und Analysen über die Fitness und die

Gesundheit des Konsumenten zusammenstellen konnten. Bis dato haben sich zahlreiche IoT-Geräte etabliert, die zunehmend eine Vermischung von

- analoger Messung
- digitaler Übermittlung
- Speicherung und
- Aggregation

von Daten ermöglichen. Diese Entwicklung bringt zugleich zahlreiche Herausforderungen bezüglich Datenschutz und Datensicherheit der Konsumenten mit sich. In den folgenden Abschnitten wird dargestellt, wie die neuen Technologien im Bereich E-Health genutzt werden können. Dabei wird auch ein Überblick über die möglichen Anwendungen für Konsumenten erstellt, deren Daten genutzt werden und zu schützen sind.

2.2 E-Health heute

2.2.1 Connected Devices

IoT-Endgeräte sind reine Clients und benötigen immer ein Zielsystem, an welches sie (drahtlos) Daten übermitteln können, die dort dann entweder aggregiert werden oder zur weiteren Verarbeitung oder Auswertung zur Verfügung stehen. Ein Gerät, das drahtlos Aufgaben erfüllt und Aktionen hervorruft, aber nicht mit einem Ziel-Serversystem verbunden wird, ist kein IoT-Gerät (z. B. Fernbedienungen, elektr. Schlüssel). Lassen sich gleiche Aktionen jedoch auch über ein Netzwerk wie das Internet steuern (z. B. Öffnung von Autos oder Garagentoren durch eine App), spricht man hierbei vom Internet of Things.

2.2.2 Kabellose Sensorik – Body Area Networks

Eine weitere und immer wichtiger werdende Klasse von medizinischen Systemen ist die der (persönlichen) elektronischen Gesundheitsvorsorge. Angesichts zunehmender Kosten medizinischer Behandlungen werden neue Geräte entwickelt, die das Wohlergehen von Einzelpersonen überwachen und im Bedarfsfall automatisch einen Arzt kontaktieren können. Bei vielen dieser Systeme besteht ein wesentliches Ziel darin, der Einweisung in ein Krankenhaus vorzubeugen.

Systeme zur persönlichen Gesundheitsvorsorge sind häufig mit verschiedenen Sensoren ausgerüstet, welche als (vorzugsweise kabelloses) BAN (Body Area Network, Körperbereichsnetzwerk) angeordnet sind. Ein wichtiger Aspekt besteht darin, dass ein solches Netzwerk eine Person möglichst gar nicht oder nur minimal behindern sollte. Zu diesem Zweck sollte das Netzwerk arbeiten können, während sich eine Person bewegt, ohne die Person mit Kabeln an unbewegliche Geräte zu binden.

Diese Anforderungen können durch zwei verschiedene Anordnungen erfüllt werden: In der ersten ist ein zentraler Hub Teil des BAN, der die benötigten Daten sammelt. Von Zeit zu Zeit werden diese Daten auf ein größeres Speichergerät heruntergeladen. Ein aktuell oft angewendetes Beispiel dafür sind Puls- und Schrittmessungen in einer Smartwatch, deren Daten auf ein Smartphone übertragen werden und auf diesem konfiguriert und verwaltet werden können. Der Vorteil dieses Verfahrens besteht darin, dass der Hub (Smartphone) das BAN (Smartwatch) verwalten kann.

Im zweiten Szenario ist das BAN über eine kabellose Verbindung kontinuierlich in ein externes Netzwerk eingebunden, an welches es die Überwachungsdaten sendet. Für die Verwaltung des BAN müssen eigene Techniken entwickelt werden. Natürlich können auch weitere Verbindungen zu Ärzten oder anderen Menschen bestehen.

Der wesentliche Unterschied besteht also darin, dass im ersten Fall der Nutzer die Messungen verwalten, administrieren und auf den Hub herunterladen kann, wohingegen im zweiten Fall die Daten über eine Schnittstelle an ein entferntes System, i. d. R. einen Server mit Datenbank-Management-System (DBMS), übertragen werden.

Aus der Sicht eines verteilten Systems, bei dem wie oben beschrieben das Management des Systems von externer Stelle betrieben werden kann, werden Firmen, die diese Technologien bereitstellen, unmittelbar mit Fragen wie den folgenden konfrontiert:

- Wo und wie sollten die Überwachungsdaten gespeichert werden?
- Wie kann man den Verlust kritischer Daten verhindern?
- Welche Infrastruktur wird benötigt, um Alarme auszulösen und weiterzuleiten?
- Wie kann das Überwachungssystem möglichst robust gestaltet werden?
- Welche Sicherheitsaspekte sind zu beachten und wie lassen sich geeignete Verfahren durchsetzen?

Im Gegensatz zu den Haussystemen, die unter eigener Kontrolle gesteuert werden, kann bei verteilten Systemen im Gesundheitswesen nicht erwartet werden, dass sie sich in Richtung von Single-Server-Systemen entwickeln und Überwachungsgeräte mit minimaler Funktionalität aufweisen werden. Im Gegenteil: Aus Gründen der Effizienz müssen Geräte und BANs die Verarbeitung im Netzwerk unterstützen. Die Überwachungsdaten müssen also beispielsweise zusammengefasst werden, bevor sie permanent gespeichert oder an einen Arzt gesendet werden. Anders als bei klassisch verteilten Informationssystemen gibt es bei BANs bisher noch keine gesicherten und nutzerfreundlichen Umsetzungsmöglichkeiten.

Ein Begriff, der BANs mit anderen Sensor- und Near-Field-Kommunikationsgeräten zusammenfasst, die Geräte über eine eigene oder eine „geliehene“ Internet-Schnittstelle mit Hubs (Smartphones/Servern) verbinden, lautet „Internet of Things“.

2.2.3 Sicherheit im Internet und Sicherheit mobiler Endgeräte als definiertes Grundbedürfnis

Die globale Verfügbarkeit des Internets führt durch drahtlose, netzwerkfähige Geräte dazu, dass Firmen die stetige Verfügbarkeit der Gerätedaten für neue Geschäftsmodelle nutzen können. Es kann heute davon ausgegangen werden, dass das Internet und mobile Endgeräte in Industrienationen in nahezu jedem Haushalt verfügbar sind. Gerade im Bezug auf vertrauliche Daten, wie es medizinische Datensätze sind, ist die Sicherheit dieser Systeme unerlässlich. Dasselbe gilt hierbei auch für die Systemstabilität, z. B. in einem Krankenhaus.

Sicherheit in einem IoT-System ist eng verwandt mit dem Begriff der Systemstabilität. Einfach ausgedrückt ist ein stabiles IoT-System eines, in das man das berechnete Vertrauen setzen kann, dass es seine Dienste leisten wird. Die Systemstabilität umfasst:

- Verfügbarkeit
- Zuverlässigkeit
- Betriebssicherheit
- Wartungsfreundlichkeit
- Vertraulichkeit
- Integrität

Vertraulichkeit (Confidentiality) bezieht sich auf die Eigenschaft eines Systems, seine Informationen nur autorisierten Parteien preiszugeben. Integrität bedeutet, dass nur autorisierte Änderungen an den Bestandteilen eines Systems vorgenommen werden können. Unzulässige Änderungen sollten sich also in einem sicheren Computersystem aufspüren und rückgängig machen lassen. Die wesentlichen Bestandteile jedes Netzwerksystems, wozu IoT-Systeme zählen, sind seine Hardware, seine Software und seine Daten.

Eine andere Sicht auf das Thema Sicherheit in einem Computersystem befasst sich mit dem Versuch, die gebotenen Dienste und Daten vor Sicherheitsbedrohungen (Security Threads) zu schützen. Vier Arten von Sicherheitsbedrohungen sind zu berücksichtigen:

- Abfangen (Interception)
- Stören (Interruption)
- Verändern (Modification)
- Einbringen (Fabrication)

Der Begriff des **Abfangens** bezieht sich darauf, dass eine unautorisierte Partei Zugriff auf einen Dienst oder auf Daten erlangt. Ein typisches Beispiel für das Abfangen ist das Abhören der Kommunikation zwischen zwei Parteien durch einen Dritten. Abfangen

liegt auch vor, wenn Daten illegal kopiert werden, z. B. nach dem Eindringen in ein privates Benutzerverzeichnis in einem Dateisystem.

Ein Beispiel für eine **Störung** ist eine beschädigte oder gelöschte Datei. Allgemeiner formuliert bezieht sich der Begriff „Störung“ auf die Situation, dass Dienste oder Daten nicht mehr verfügbar, nicht mehr verwendbar oder zerstört sind. In diesem Sinne sind DoS-Angriffe (Denial of Service), durch die jemand in böswilliger Absicht versucht, den Zugriff anderer auf einen bestimmten Dienst zu verhindern, eine Sicherheitsbedrohung, die als Störung zu klassifizieren ist.

Abänderungen bedeuten unautorisierte Änderungen an Daten oder Manipulationen an einem Dienst mit der Folge, dass dieser von seinen ursprünglichen Spezifikationen abweicht. Beispiele für Änderungen umfassen das Abfangen und nachfolgende Abändern von übermittelten Daten, Manipulationen an Datenbankeinträgen und das Ändern eines Programms in der Weise, dass es insgeheim die Aktivitäten seines Benutzers aufzeichnet.

Eine **Fälschung** liegt vor, wenn zusätzliche Daten oder Aktivitäten erzeugt werden, die es normalerweise gar nicht gäbe. Ein Eindringling könnte z. B. versuchen, einen Eintrag zu einer Passwortdatei oder einer Datenbank hinzuzufügen. Genauso ist es manchmal möglich, in ein System einzudringen, indem zuvor gesendete Nachrichten, wie abgefangene Log-in-Requests, wiederholt abgespielt werden, um als Antwort des Ziel-servers einen erfolgreichen Log-in zu erhalten und auf diese Weise auf diverse Daten zugreifen zu können.

Es ist stets wichtig zu bedenken, dass Störungen, Abänderungen und Fälschungen jeweils als Form der Datenverfälschung betrachtet werden können. Nur festzuhalten, dass ein System in der Lage sein sollte, sich selbst gegen alle möglichen Sicherheitsbedrohungen zu schützen, genügt nicht, um ein tatsächlich sicheres System einzurichten. Was zunächst benötigt wird ist eine Beschreibung der Sicherheitsanforderungen, also Sicherheitsrichtlinien. Sicherheitsrichtlinien beschreiben im Detail, zu welchen Aktionen die Entitäten in einem System befugt sind und welche verboten sind.

Entitäten umfassen z. B.:

- Benutzer
- Dienste
- Daten
- Rechner

Sind einmal Sicherheitsrichtlinien niedergelegt worden, wird es möglich, sich auf die Sicherheitsmechanismen zu konzentrieren, durch die sie durchgesetzt werden können. Wichtige Sicherheitsmechanismen sind die folgenden:

- Verschlüsselung
- Authentifizierung
- Autorisierung
- Kontrolle

Verschlüsselung ist grundlegend für die Computersicherheit. Eine Verschlüsselung wandelt Daten in etwas um, das ein Angreifer nicht verstehen kann. Verschlüsselung bietet also ein Mittel zur Umsetzung von Datenvertraulichkeit. Zudem ermöglicht Verschlüsselung die Überprüfung, ob Daten modifiziert worden sind. Sie unterstützt damit die Überprüfung der Integrität.

Authentifizierung wird verwendet, um die behauptete Identität eines Benutzers, Clients, Servers, Hosts oder einer anderen Entität zu überprüfen. Bei Clients gilt als grundlegende Voraussetzung, dass ein Dienst die Identität eines Clients in Erfahrung bringen muss, bevor er in seinem Auftrag in irgendeiner Weise tätig wird (außer der Dienst steht jedem zur Verfügung). Benutzer werden im Normalfall durch Passwörter authentifiziert, aber es gibt viele andere Möglichkeiten, Clients zu authentifizieren.

Nach der Authentifizierung eines Clients ist es erforderlich zu prüfen, ob dieser Client **autorisiert** ist, die angefragte Aktion auszuführen. Der Zugriff auf Datensätze in einer medizinischen Datenbank ist ein typisches Beispiel. Je nachdem, wer auf die Datenbank zugreift, kann die Erlaubnis für das Lesen der Datensätze, das Ändern bestimmter Felder in einem Datensatz oder das Hinzufügen oder Löschen eines Datensatzes gewährt werden.

Kontrollwerkzeuge werden zur Nachverfolgung verwendet, welche Clients worauf zugegriffen haben und in welcher Weise. Auch wenn Kontrollen keinen wirklichen Schutz vor Sicherheitsbedrohungen bieten, können Kontrollprotokolle äußerst nützlich für die Analyse eines Sicherheitsbruches und die nachfolgende Einleitung von Maßnahmen gegen Eindringlinge sein. Aus diesem Grund sind Angreifer normalerweise begierig, keine Spuren zu hinterlassen, die letztendlich zur Aufdeckung ihrer Identität führen könnten. Das Protokollieren von Zugriffen führt so dazu, dass Angriffe ein riskanteres Unternehmen werden.

2.3 Mögliche zukünftige Entwicklungen

Aufgrund der schnelleren Übertragungsgeschwindigkeiten drahtloser Kommunikationsmedien und leistungsfähigeren Speicher sind die Möglichkeiten, multiple Messdaten zeitgleich in einer genaueren Art und Weise von IoT-Geräten zu senden und zu empfangen, sehr weitreichend.

Besonders in den Bereichen Connected Home bz. Ambient Assisted Living und E-Health sind sensorgestützte Geräte, welche über das WLAN oder eine SIM-Karte im direkten Austausch mit dem Internet kommunizieren, ein stetig wachsender Markt.

Durch die immer günstiger werdenden Kleinstspeicher wird sich der IoT-Markt auch der Open-Source-Community öffnen, was wahrscheinlich zu einer dezentralen Entwicklung führen wird, die keiner Überwachung unterliegt. Ob dies eine positive oder negative Entwicklung ist, wird sich zeigen, jedoch ist die Anforderung an Sicherheit gerade in dezentralen Strukturen das oberste Gut.

Einen weiteren wichtigen Punkt stellt die asymmetrische Verschlüsselung dar, welche aktuell auf physikalische Grenzen stößt.

Verfahren, die auf asymmetrischer Verschlüsselung beruhen, um Datensätze zu schützen, sind in vielen Sensornetzen nicht nutzbar, da sie hohe Ansprüche an Rechenleistung und Speicherplatz stellen. Aktuell bieten IoT-Geräte nur eine sehr geringe Rechenleistung.³ Durch zunehmend energiesparendere Verfahren und leistungsstärkere Nano-Prozessoren können IoT-Geräte jedoch in Zukunft vermutlich auch asymmetrische Verschlüsselungen anwenden. Bis dahin müssen ggf. Prozessoren des Wirtsystems genutzt werden (PC, Smartphone).

2.4 Fehldiagnosen und Haftungsfragen

Die Möglichkeit, automatisiert Diagnosen zu erstellen, birgt zugleich das Risiko von Fehldiagnosen durch vorsätzliche Manipulation oder technische Sicherheitslücken (Exploits). Im IoT-Bereich besteht durch die Peripherie bedingt die Gefahr, dass eine Sicherheitslücke nicht unmittelbar bei Bekanntwerden geschlossen werden kann: Klassische Software kann durch den Download eines Patches die Schließung einer Sicherheitslücke gewährleisten. Hardware hingegen benötigt ein sogenanntes Firmware-Update bzw. ein Update der in der Hardware eingesetzten Software. Sollte die Sicherheitslücke die Hardware direkt betreffen, ist ein Firmware-Update nicht möglich. Das IoT-Gerät müsste dann entweder durch ein anderes ersetzt oder nach einer Rückrufaktion hardwaretechnisch verbessert werden. Aus diesem Grund ist das Sicherheitsmanagement schon in der Konzeptphase des Gerätes anzuwenden. Normen in Form von begleitenden Kriterienkatalogen sind daher zu empfehlen.

Als Beispiel für eine Fehldiagnose kann eine Peripherie herangezogen werden, welche den Glukosespiegel einer diabeteskranken Person misst. Durch einen Messfehler kann hierbei eine potenziell lebensbedrohliche Situation hervorgerufen werden. Dieser Messfehler kann durch Produktionsfehler bei der Herstellung des IoT-Gerätes, durch eine Manipulation des Datenverkehrs, durch eine Manipulation der Hardware oder durch einen Programmierfehler auftreten. Nutzt ein potenzieller Angreifer eine grob fahrlässige Sicherheitslücke aus, um den Datenverkehr der Messung zu manipulieren, wobei eine Person zu Schaden kommt, ist ohne die Kenntnis der Sicherheitslücke nicht nachzuweisen, wodurch der Messfehler verursacht wurde. Aus diesem Grund ist die Zuweisung der Haftungsspflicht im Falle eines Personenschadens nicht ohne zusätzliches Wissen möglich. Sollte ein IoT-Gerät z. B. anhand eines vordefinierten Kriterienkataloges konzipiert und durch eine unabhängige dritte Instanz geprüft worden sein, kann ein Verschulden der IoT-Anbieter teilweise ausgeschlossen werden und das Prüfergebnis im Falle eines Rechtsstreits herangezogen werden. Ein Eigenverschulden des IoT-Nutzers kann somit in Betracht gezogen werden.

³Schmidt (2003).

Im Gegensatz zu vielen klassischen IT-Systemen, die in ihrem Aufbau vor dem physischen Zugriff durch unautorisierte Personen geschützt sind, werden Sensorknoten, wie sie im IoT-Bereich vorkommen, in Umgebungen eingesetzt, in denen in aller Regel physischer Zugang zu den Sensorknoten möglich ist und damit leicht funktionale Beeinträchtigungen eines Sensorknotens realisierbar wären. Aufgrund der geringen Sendeleistung der IoT-Geräte (unmittelbare Nähe) ist es möglich, den Funkkanal mittels elektromagnetischer Einstrahlung zu stören. Auch sind bei Ad-hoc-Netzen und im Besonderen bei Sensornetzwerken spezielle Angriffe auf den verschiedenen Protokollebenen bekannt. Darüber hinaus sind im Gegensatz zu klassischen Kommunikationsnetzwerken die eigentliche Anwendung und die Funktion des Kommunikationsnetzwerkes auch noch stark ineinander verwoben. Zusammengenommen stellt die sichere Konfiguration eines Sensornetzwerkes eine große Herausforderung dar⁴.

Bei der Konzeption des IoT-Gerätes ist zudem darauf zu achten, dass eine Manipulation der Hardware weitestgehend erschwert wird. Dies kann z. B. durch Gehäuse aus einem Guss erfolgen. Eine Isolation gegen gezielte elektromagnetische Störsignale ist nicht möglich. Die Funktionalität sollte in einem solchen Fall jedoch eingeschränkt oder blockiert werden.

Literatur

Schmidt, Stefan/ Buschmann, Carsten/Fischer, Stefan (2003): Sicherheit in Sensornetzen am Beispiel von Swarms; erschienen in 1. GI/ITG Fachgespräch Sensornetze, Technical Report 2003. Zitieren als: Schmidt 2003.

⁴BSI Sensornetzwerken.

E-Health: Datenschutz und Datensicherheit
Herausforderungen und Lösungen im IoT-Zeitalter

Bauer, C.; Eickmeier, F.; Eckard, M.

2018, VIII, 160 S. 13 Abb., Softcover

ISBN: 978-3-658-15090-7