

# Aktuelle und zukünftige Sicherheitsbedrohungen für medizinische Geräte und Systeme



Das Internet der Dinge (IoT) ist in zahlreichen Branchen vertreten, die Gesundheitsbranche bildet dabei keine Ausnahme. Vernetzte medizinische Geräte und Systeme, die wichtige Gesundheitsdaten sammeln, übertragen und speichern können, eröffnen neue Möglichkeiten der Patientenüberwachung und medizinischen Ferndiagnose. So helfen diese Lösungen dabei, Herausforderungen, wie Personalmangel und steigende Gesundheitskosten, durch schnellere Diagnose und Behandlung zu bewältigen und bieten gleichzeitig mehr Komfort für die Patienten. Angesichts dieser Perspektiven wird erwartet, dass der weltweite Markt für Medizinprodukte von 455,34 Mrd. USD im Jahr 2021 auf 657,98 Mrd. USD im Jahr 2028 wächst [1]. Das stellt ein enormes Potenzial für Entwickler und Hersteller dar, bringt jedoch auch große Herausforderungen mit sich. Die offensichtlichste und am häufigsten diskutierte, ist die Sicherheit – zumal Sicherheitslücken in einem an ein Netzwerk angeschlossenen Gerät Cyberkriminellen ein Tor zu einem viel umfangreicheren Netzwerk öffnen können. R&D-Spezialist Bittium beleuchtet aktuelle

und zukünftige Hauptbedrohungen, die Systemdesigner berücksichtigen sollten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat kürzlich untersucht, inwieweit Medizinprodukte von Cyberangriffen gefährdet sind [2]. Die Experten überprüften verschiedene Medizinprodukte zur Behandlung und Versorgung von Patienten hinsichtlich ihrer IT-Sicherheit – darunter zufällig ausgewählte Herzschrittmacher, Defibrillatoren, Insulinpumpen, Beatmungsgeräte, Infusionspumpen, Patientenmonitore und Heimnotrufsysteme für Senioren, die häufig in der Pflege und Betreuung eingesetzt werden. Sie fanden rund 150 Schwachstellen. Damit steigt das Risiko für Krankenhäuser und andere Gesundheits- oder Pflegeeinrichtungen: Eine nicht gepatchte Sicherheitslücke in einem einzigen Gerät reicht aus, um das gesamte Netzwerk zu kompromittieren, da sich Cyberkriminelle Schritt für Schritt in ein Netzwerk einarbeiten können. Bei einem Ransomware-Angriff auf das Universitätsklinikum Düsseldorf im vergangenen September wurde die Schadsoftware höchstwahrscheinlich nach

Bekanntwerden eines Sicherheitsmangels und vor Bereitstellung eines Patches blieb monatelang unbemerkt und verbreitete sich im gesamten IT-Netzwerk.

Bereits heute muss jedes Medizinprodukt mindestens 5-10 Sicherheitsstandards erfüllen, darunter beispielsweise mehrere ANSI/AAMI MEE-Standards, IEC-Standards oder AIM-Standards. Zudem entwickeln sich auch diese Standards ständig weiter, um die Cybersicherheit zu berücksichtigen.

## Persönlich identifizierbare Informationen (PII) in Gefahr

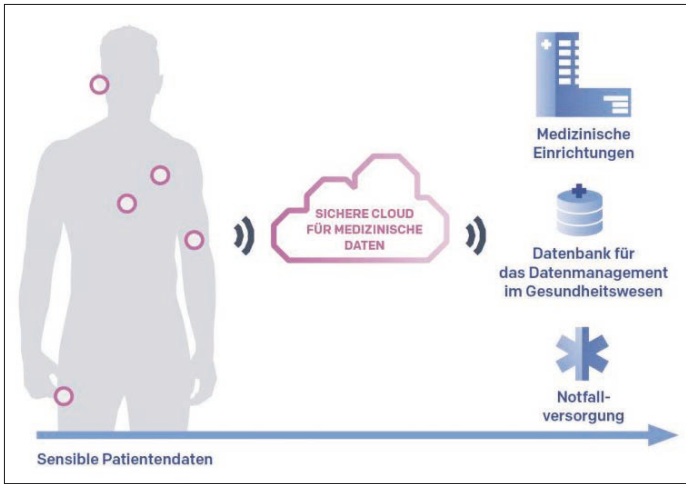
Eines der wichtigsten Sicherheitsrisiken ist der Umgang mit personenbezogenen Daten (PII). Derzeit werden Medizinprodukte oft nicht als Produkte angesehen, die PII enthalten und übertragen könnten. Daher werden die gesammelten und in die Cloud oder ein Netzwerk übertragenen Daten nicht gemäß den Regeln der EU-Datenschutzgrundverordnung (DSGVO), des California Consumer Privacy Act (CCPA) oder des Health Insurance Portability and Accountability Act (HIPAA) behandelt. Diese Vorgaben spezifizieren, wie PII-Daten aufgrund spezifischer Vorschriften in Bezug auf die Datennutzung gesichert, gespeichert und sogar professionell vernichtet werden müssen.

Selbst wenn Daten, die PII enthalten können, nach der Verwendung vom medizinischen Gerät selbst gelöscht werden, können die Informationen oft in einem Netzwerk oder in einer Cloud-Umgebung verbleiben. Dies kann einerseits zu zukünftigen Compliance-Problemen führen, wenn die DSGVO- und/oder CCPA-Vorschriften auf Medizinprodukte in dem sich schnell entwickelnden Markt für das medizinische Internet der Dinge (MIoT) angewendet werden. Andererseits öffnen die ungesicherten Daten die Türen für zusätzliche zukünftige Sicherheitsbedrohungen.



*Autor:  
Hannu Juopperi  
Sicherheitsarchitekt*

*Bittium Corporation  
www.bittium.com*



## Medizinische Daten fälschen und für Cyberangriffe nutzen

Da immer mehr medizinische Daten über IoT-Geräte gesammelt werden, muss auf jeden Fall gewährleistet werden, dass die Informationen korrekt sind. Das bedeutet, dass die Daten während der Übertragung und im Ruhezustand gesichert werden müssen, um dafür zu sorgen, dass das Gerät nicht kompromittiert wird. Das gilt nicht nur für PII-Daten, sondern für alle Daten, die von Medizinprodukten erfasst werden.

Wenn diese Daten nicht korrekt gesichert sind, könnten die gesammelten medizinischen Informationen selbst für Angriffe verwendet werden. Bei einem Replay-Angriff könnten beispielsweise medizinische Daten an die medizinische Behörde zurückgespielt und dadurch die aktuelle medizinische Datensammlung verfälscht werden.

Das bedeutet ein zweifaches Risiko: Einerseits könnte dies für eine Denial-of-Service-Attacke (DoS) genutzt werden, um einen medizinischen Leistungserbringer oder eine medizinische Behörde handlungsunfähig zu machen. Andererseits stellt dies eine ernsthafte Gefahr für die Gesundheit von Patienten dar, da der behandelnde

Arzt keine Kenntnis über die aktuelle Situation/den aktuellen medizinischen Status seiner Patienten hat.

## Biometrische Authentifizierung

Authentifizierungen durch Fingerabdrücke, Gesichtserkennung oder Iris-Scans gelten als besonders sicher und werden auch in der Multi-Faktor-Authentifizierung verwendet. Zum Einsatz kommen sie u.a., um den Zugang zu Gebäuden, Autos, mobilen Geräten oder Daten abzusichern. Wenn es um die Erfassung hochsensibler Gesundheitsinformationen durch medizinische Geräte und Wearables geht, schlagen Experten von Ingenieur- und Technologieverbänden wie dem IEEE vor, biometrische Authentifizierung zu verwenden, um die Nutzung und den Zugriff zu sichern [3]. Weitere Vorteile wären, dass ein intelligentes Endgerät („Smart Device“) den Benutzer erkennt und das Serviceprofil anpassen kann – genau wie Autos der neuesten Generation den Fahrer durch biometrische Erkennung identifizieren und Sitz- sowie Airbag-Positionen für die Sicherheit anpassen oder den Zugriff auf persönliche Informationen über das Infotainment-System ermöglichen, usw..

Auf der anderen Seite könnten in Zukunft auch Biosignale selbst

missbraucht werden. Durch die Erhebung medizinischer Daten über einen längeren Zeitraum können Informationsprofile erstellt werden, mit denen eine Person identifiziert werden kann. Das mag nach Science-Fiction klingen, aber es gibt mehrere Studien zur Verwendung von EKG-Profilen als Grundlage zur Identifikation von Einzelpersonen [4]. Laut einem Bericht des MIT Technology Review testet das Pentagon bereits einen Laser, der Menschen anhand ihres Herzschlags identifizieren kann [5]. Andere biometrische Techniken wie die Ganganalyse („Gait Analysis“), die Personen anhand ihres Gangs identifiziert, wurden verwendet, um berüchtigte Terroristen vor einem Drohnenangriff zu identifizieren. Aber die Art, wie wir uns bewegen, ist, ebenso wie die Gesichtserkennung, nicht immer unverwechselbar genug für eine sichere Identifizierung. Die Herzsignatur einer Person ist jedoch einzigartig, wie eine Iris oder ein Fingerabdruck. Und obwohl es zweifellos legitime Szenarien gibt, eine Herzsignatur als Identifikator zu verwenden, gibt es leider auch Möglichkeiten, diese Informationen zu missbrauchen. Dies bringt uns zurück zu der Überlegung, warum medizinische Daten mit den höchsten Sicherheitsstandards behandelt werden müssen.

## Individueller Ansatz erforderlich

Mit der weltweiten Zunahme von IoT- und MIIOT-Geräten (tragbare und miteinander verbundene medizinische Objekte, die eine Fernüberwachung des Gesundheitszustands ermöglichen) sind sich alle Experten einig, dass die Sicherheitsmaßnahmen verbessert werden müssen. Gesundheitsdaten sind hochsensibel und ziehen die Aufmerksamkeit von

Angriffern auf sich [6]. Medizinprodukte sind ein lohnendes Ziel für Hacker, da sie in der Regel leicht zu kapern sind [7]. Ein Grund für ihre Anfälligkeit ist die vergleichsweise lange Lebensdauer der Geräte. Da Medizinprodukte lange Zertifizierungsprozesse durchlaufen müssen, werden zu Beginn des Zertifizierungsprozesses häufig Konfigurationseinstellungen auf der verwendeten Firmware- und Betriebssystemversion eingefroren. Entwickler müssen einen Weg finden, die Sicherheitsmaßnahmen während der Lebensdauer des Geräts zu aktualisieren, ohne die Zertifizierungen zu beeinträchtigen.

„Ein offensichtlicher Schritt in die richtige Richtung ist, dass Gesundheitsdaten daher in den Geltungsbereich von DSGVO, CCPA oder HIPAA fallen müssen. Hersteller und Geräteentwickler müssen verstehen, dass die Daten PII sind und als solche behandelt werden müssen“, erklärt Lösungsarchitekt Hannu Juopperi von Bittium. „Andere nützliche Ansätze umfassen die Implementierung des Sicherheitsbedrohungsmodells „STRIDE“ – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service und Elevation of Privilege. Aufgrund unterschiedlicher Konstruktionen und Anwendungsarten von Medizinprodukten gibt es jedoch keinen einheitlichen Weg, um alle notwendigen Sicherheitsmaßnahmen zu implementieren. Jedes Gerät muss individuell hinsichtlich der medizinischen Datensicherheit bewertet werden. Wenn ein Hersteller von Medizinprodukten oder ein Entwickler-Team nicht über die erforderliche Expertise im Bereich Forschung und Entwicklung (F&E) oder die Testeinrichtungen im eigenen Haus verfügt, kann sich die Zusammenarbeit mit einem F&E-Spezialisten mit dem erforderlichen Know-how rentieren.“ ◀

## Quellen:

- [1] <https://www.fortunebusinessinsights.com/industry-reports/medical-devices-market-100085>
- [2] [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/ManiMed\\_Abschlussbericht.pdf?\\_\\_blob=publicationFile&v=1](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/ManiMed_Abschlussbericht.pdf?__blob=publicationFile&v=1)
- [3] Bio-signals for secure authentication (IEEE) <https://par.nsf.gov/servlets/purl/10108265>
- [4] ECG profiles as identifier <https://biomedical-engineering-online.biomedcentral.com/articles/10.1186/s12938-015-0072-y>
- [5] MIT Technology Review: <https://www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distance-by-their-heartbeat/>
- [6] <https://owasp.org/> - <https://www.hindawi.com/journals/jhe/2021/6632599/>
- [7] [https://www.researchgate.net/publication/314089398\\_Broken\\_Hearted\\_How\\_To\\_Attack\\_ECG\\_Biometrics](https://www.researchgate.net/publication/314089398_Broken_Hearted_How_To_Attack_ECG_Biometrics)