Cybersecurity in Connected Healthcare: Socio-Technical Interactions within the Internet of Medical Things (IoMT)

Grigori Rogge

Lehrstuhl für Management und Innovation im Gesundheitswesen
Fakultät für Wirtschaft und Gesellschaft, Universität Witten/Herdecke, Witten

Cybersecurity im Kontext des Gesundheitswesens

Krankenhäuser gelten als zentraler Teil der kritischen Infrastruktur und gehören zum Gesundheitswesen. Die Digitalisierung dieses Bereichs führt zu einer höheren Verfügbarkeit von Gesundheitsdaten, die genutzt werden können, um mehr Effizienz und Transparenz in der Patientenbehandlung zu gewährleisten [1].

Ein wichtiger Teilbereich der Digitalisierung ist das Internet of Medical Things (IoMT). Im IoMT sind verschiedene medizinische Geräte und Anwendungen, wie beispielsweise Sensoren für Gesundheitsdaten und Patientendatenmanagementsysteme, miteinander vernetzt. Dadurch können Vitalparameter automatisch überwacht, Medikationen gezielt eingestellt und potenzielle Kontraindikationen erkannt werden [2].

Durch die erhöhte Digitalisierung ist die Anzahl potenzieller Zugangspunkte in die Systeme der Gesundheitsbranche sowie die Menge der verarbeiteten Daten stark angestiegen. Gesundheitsdaten machten 2023 etwa 30 Prozent des weltweiten Datenverkehrs aus [3].

Gesundheitsdaten enthalten verschiedenste persönliche Informationen und gelten als besonders wertvoll. Dies sowie die hohe Bedeutung des Gesundheitswesens führt zu einer hohen Bedrohung durch Cyberkriminelle [4].

Zwischen Januar 2021 und März 2023 entfielen 53 Prozent der Cyberattacken in Europa auf Gesundheitseinrichtungen. Ein Großteil dieser Attacken (42 Prozent) ereignete sich in Krankenhäusern [5]. Dabei werden veraltete Soft- und Hardware, ein Ausbleiben von Investitionen sowie der Mensch als Unsicherheitsfaktor ausgenutzt [6].

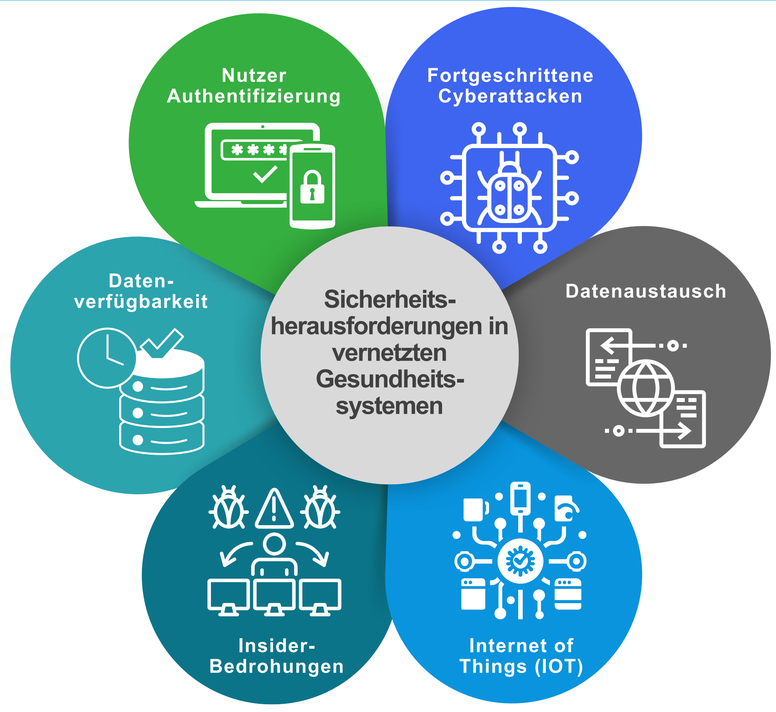

Abb. 1: Potenzielle Cyber-Gefährdungen

Stand der aktuellen Forschung zu Cybersecurity

Cybersecurity ist ein prominentes Thema in der aktuellen Forschung. Ein Teilbereich ist die Cybersecurity des Internet of Medical Things (IoMT) [7, 8]. Dabei werden besonders der Einsatz von Technologien wie Blockchain, Machine Learning (ML) und Artificial Intelligence (AI) diskutiert, um IoMT-Netzwerke besser vor Cyberangriffen zu schützen [7, 8]. In diesem Zusammenhang geht es insbesondere darum, dass z. B. Blockchain die Möglichkeit bietet, Daten besser zu verschlüsseln, oder dass durch den Einsatz von AI bzw. ML leistungsstärkere Systeme zur Erkennung von Cyberangriffen entwickelt werden können.

Ein im Kontext von Cybersecurity ebenfalls zu berücksichtigender Aspekt ist der menschliche Faktor. Aktuelle Studien diskutieren die Notwendigkeit, den menschlichen Faktor stärker beim Risikomanagement sowie bei der Entwicklung von vernetzten Gesundheitssystemen zu berücksichtigen. In diesem Zusammenhang wird die Notwendigkeit einer sozio-technischen Perspektive hervorgehoben [9, 10]. Zudem wird beschrieben, dass der Einfluss von organisationalen Maßnahmen im Bereich Cybersecurity bisher nicht ausreichend erforscht ist.

Promotionsvorhaben

Das kumulative Promotionsvorhaben besteht aus drei sequenziell aufgebauten Teilen, die unterschiedliche Schwerpunkte setzen und einen Überblick über die sozio-technischen Interaktionen im IoMT geben sollen. In der Makroperspektive wird zunächst untersucht, welche sozio-technischen Interaktionen im Rahmen vernetzter Gesundheitssysteme stattfinden und welche Cyberrisiken hieraus entstehen. Anschließend wird auf der Mikroebene geprüft, wie sich medizinisches Personal in cybersicherheitskritischen Situationen verhält. Schließlich wird das Verständnis um die Herstellerperspektive erweitert und nachvollzogen, wie Hersteller von IoMT-Systemen sozio-technische Anforderungen und organisationale Aspekte bei der Implementierung von IoMT-Systemen berücksichtigen.

Durch das Forschungsvorhaben wird ein holistisches Verständnis der sozio-technischen Interaktionen und IT-Risiken in vernetzten Gesundheitssystemen geschaffen. Gleichzeitig wird untersucht, wie die resultierenden Anforderungen in die Implementierung und das Design von vernetzten Gesundheitslösungen integriert und berücksichtigt werden können.

Schritt 1: Reported Incidents and Expert Assessments: A Mixed-Methods Study

An dieser Studie wird seit Beginn des Jahres 2025 gearbeitet und es ist geplant, die Arbeit bis Oktober 2025 abzuschließen.
Bei der Methodik der Studie handelt es sich um einen Mixed-Methods-Ansatz. Es werden sowohl quantitative Daten (gemeldete Cybersecurity-Zwischenfälle aus Datenbanken) als auch qualitative Daten (Experteneinschätzungen aus Fokusgruppen) gesammelt (siehe Abb. 2). Die quantitativen Daten werden als Diskussionsgrundlage für die Fokusgruppen genutzt.
Dabei geht es darum, zu verstehen, wie die Einschätzungen von IT-Experten aus deutschen Krankenhäusern die gemeldete Cybersecurity-Situation in einen Kontext setzen. Dies ist insbesondere wichtig, da die gemeldeten Daten oft generisch sind und es dadurch schwierig ist, Rückschlüsse auf genaue Risiken zu ziehen.
Die Ergebnisse der Studie sollen dazu beitragen, die Cybersecurity-Situation in deutschen Krankenhäusern zu beschreiben und zu analysieren, wie sich diese von den allgemein gemeldeten Zwischenfällen unterscheidet. Insbesondere soll erforscht werden, in welchen Situationen medizinisches Personal von vorgegebenen Cybersecurity-Richtlinien abweicht, um Patienten zu versorgen oder Prozesse zu vereinfachen.

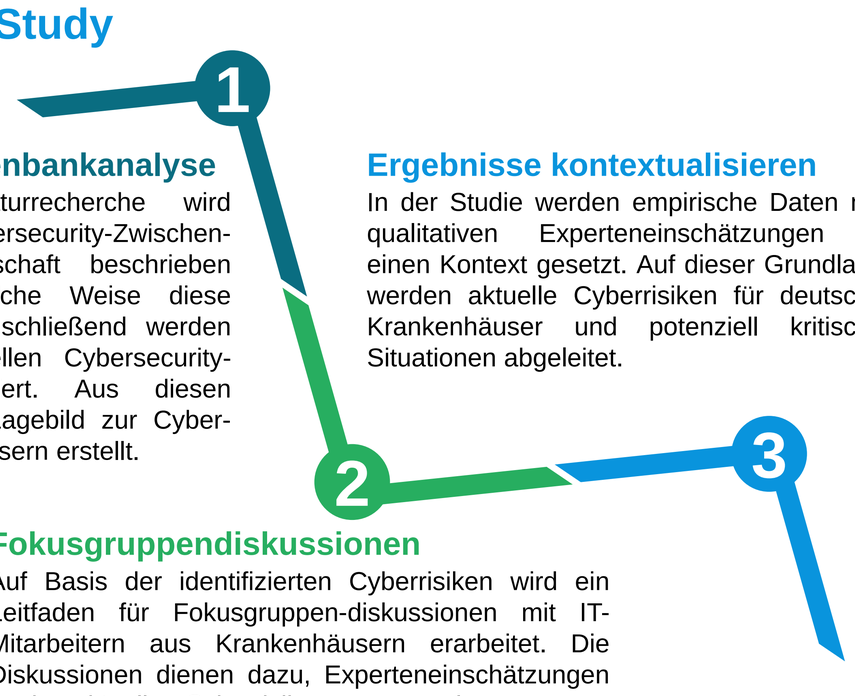

Abb. 2: Methodik der Studie

Literatur

[1] Yeung AWK, Torkamani A, Butte AJ, Glicksberg BS, Schuller B, Rodriguez B et al. The promise of digital healthcare technologies. Frontiers in public health 2023; doi: 10.3389/fpubh.2023.1196596

[2] Singh J. Challenges with Medical Devices Connected To Hospital Network. International Journal for Research in Applied Science and Engineering Technology 2024; doi: 10.22214/ijraset.2024.63187

[3] Boehncke K, Duprac G, Sparey J, Valente A. Tapping Into New Potential: Realising the Value of Data in the Healthcare Sector 2023; Abrufbar hier: https://www.lek.com/insights/hea/eu/ei/tapping-new-potential-realising-value-data-healthcare-sector

[4] Frith KH. Data Breaches in Health Care: Preparing Students to Avoid Unsafe Practices. Nursing education perspectives 2019; doi: 10.1097/01.NEP.0000000000000595

[5] Theocharidou M, Lella I. ENISA threat landscape report: Health sector (January 2021 to March 2023). Heraklion: ENISA 2023; Abrufbar hier: https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

[6] Cartwright AJ. The elephant in the room: cybersecurity in healthcare. Journal of clinical monitoring and computing 2023; doi: 10.1007/s10877-023-01013-5

[7] Mazhar T, Talpur DB, Shloul TA, Ghadi YY, Haq I, Ullah I et al. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain sciences 2023; doi: 10.3390/brainsci13040683

[8] Messinis S, Temenos N, Protonotarios NE, Rallis I, Kalogeras D, Doulamis N. Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. Computers in biology and medicine 2024; doi: 10.1016/j.compbiomed.2024.108036

[9] Ewoh P, Vartiainen T. Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. Journal of medical Internet research 2024; doi: 10.2196/46904

[10] Svandova K, Smutny Z. Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review. Journal of multidisciplinary healthcare 2024; doi: 10.2147/JMDH.S459987

Grigori.Rogge@uni-wh.de
www.atlas-digitale-gesundheitswirtschaft.de
www.uni-wh.de/mig

Gefördert durch das Land Nordrhein Westfalen