Herausforderungen für die Cybersicherheit in Krankenhäusern:

Analyse internationaler Vorfallberichte und Validierung durch Experten

Grigori Rogge und Sabine Bohnet-Joschko

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

universität Witten/Herdecke

Hintergrund

Die zunehmende Digitalisierung im Gesundheitswesen führt zu einer wachsenden Verarbeitung von Patientendaten und einer stärkeren Vernetzung von Geräten mit Krankenhaussystemen, wodurch sowohl die technologische Abhängigkeit als auch die Angriffsfläche für Cyberangriffe steigen [1, 2]. Infolgedessen ist der Gesundheitssektor, insbesondere Krankenhäuser, zu einem zentralen Ziel von Cyberkriminellen geworden [3].

Gleichzeitig besteht ein Mangel an öffentlich verfügbaren Daten zu Cyber- und Datenschutzvorfällen. Verfügbare Datensätze weisen häufig einen starken US-Fokus auf, zudem sind Vorfallbeschreibungen oft ungenau, was ihre Nutzbarkeit im Risikomanagement einschränkt [4, 5, 6].

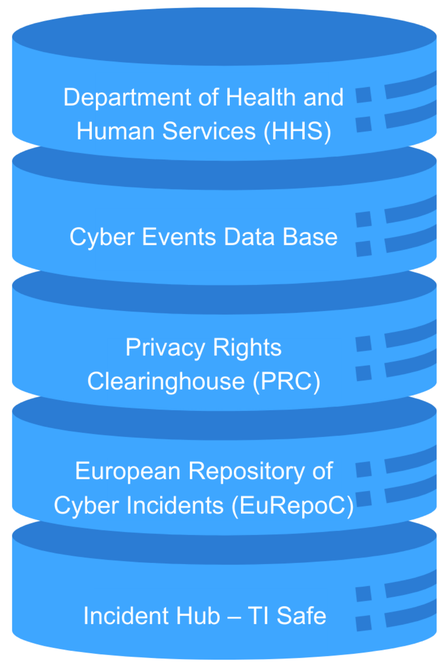
Ziel

Ziel der Studie ist es, einen holistischen Überblick über Cyberrisiken in Krankenhäusern zu schaffen, Einflussfaktoren entlang der Dimensionen des HOT-fit Modells zu identifizieren und zu untersuchen, inwiefern qualitative Experteneinschätzungen öffentliche Daten kontextualisieren oder davon abweichen.

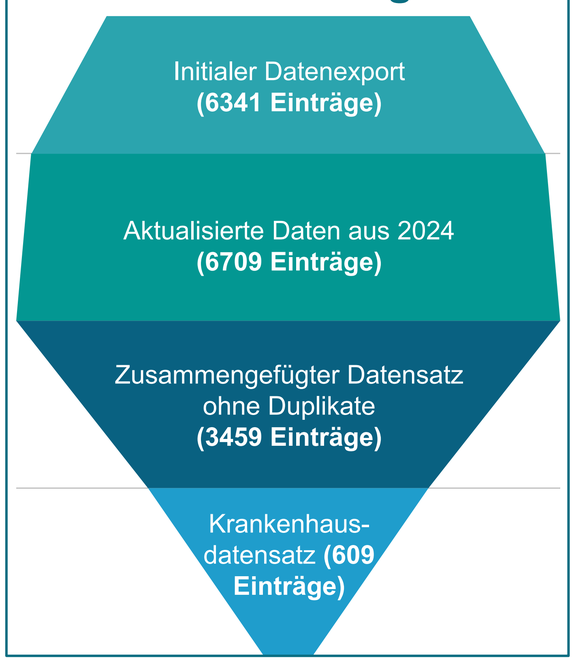
Methodik

Fünf internationale Datenbanken zu Cyber- und Datenschutzvorfällen im Gesundheitswesen wurden mithilfe eines einheitlichen Kategoriensystems zu einem Datensatz zusammengeführt und bereinigt. Auf dieser Basis wurde ein spezifischer Datensatz für Krankenhäuser erstellt. Beide Datensätze wurden deskriptiv analysiert.

Ergänzend fanden vier Fokusgruppendiskussionen mit 14 IT-Leitern und Informationssicherheitsbeauftragten aus deutschen Krankenhäusern verschiedener Größen statt, um die Ergebnisse zu kontextualisieren und zentrale Einflussfaktoren der aktuellen Risikosituation herauszuarbeiten.

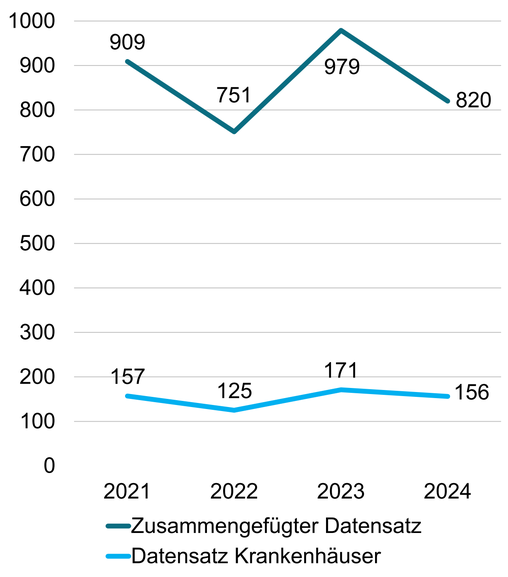


Datenvorbereitung

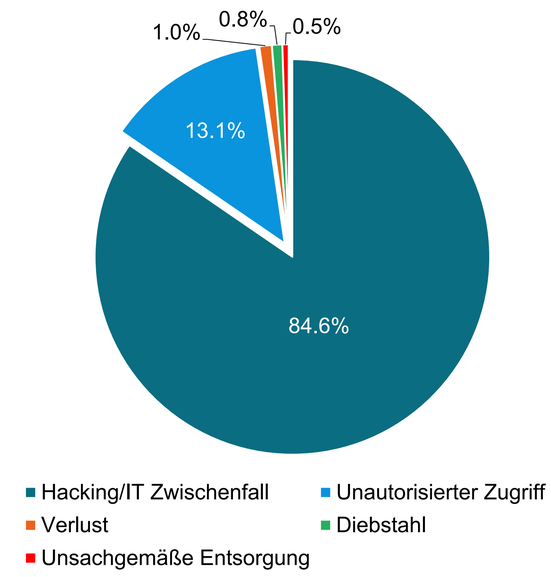


Deskriptive Datenbankanalyse

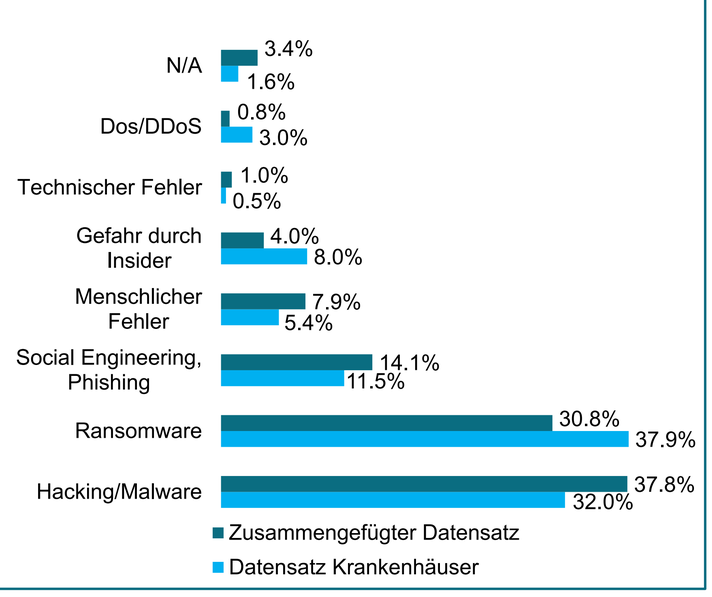
Verteilung Vorfälle nach Jahren



Verteilung nach Hauptkategorien



Verteilung nach Subkategorien



Fokusgruppendiskussionen

Die Fokusgruppendiskussionen wurden mittels thematischer Analyse nach Braun & Clarke ausgewertet, wobei die identifizierten Themen den Dimensionen des HOT-fit Modells zugeordnet wurden. Krankenhäuser stehen vor der Herausforderung, mit begrenzten Ressourcen neue Technologien zu integrieren, Nutzeranforderungen zu erfüllen und gleichzeitig interne sowie gesetzliche Sicherheitsvorgaben einzuhalten.

Neben zunehmenden Bedrohungen, etwa durch besser organisierte Angreifer oder Abhängigkeiten von externen Dienstleistern, zeigen sich auch positive Entwicklungen. Ein gesteigertes Sicherheitsbewusstsein der Mitarbeitenden ist erkennbar, während verbesserte Schutzmaßnahmen, trotz weiterhin begrenzter Datenlage, zu einer höheren Transparenz der aktuellen Risikosituation beitragen.

Technologische Faktoren bei IT-Risiken in Krankenhäusern

Sich entwickelnde Hacking-Formen
- Einsatz von KI in Hacking

Nutzbarkeit und Sicherheit balancieren
- Technologie muss sich an die Realität der Nutzer anpassen

Technische Schwachstellen
- Alte Nutzerkonten, retrospektive Integration von Maßnahmen

Neue Geräte und Software erhöhen Sicherheitsrisiken
- Unzureichende Sicherheitsarchitektur (insbesondere Medizinprodukte), Zugangsrechte Dritter,

Technische Maßnahmen, um Sicherheit zu erhöhen
- SIEM-Systeme, Netzwerksegmentierung, sichere Geräte

Organisationale Faktoren bei IT-Risiken in Krankenhäusern

Fehlende Daten für Risikomanagement und organisationales Lernen
- Informelle Quellen, Variation im Lernprozess, Kein Teilen von Daten

Sicherheitsherausforderungen im Zusammenhang mit Zulieferern
- Zugang zu Versicherungen, Ausweitung von Sicherheitsprozessen

Fehlende Expertise und Kapazität
- Fehlende physische Maßnahmen, Outsourcing, Probleme akzeptieren

Institutionalisierung von Hacking
- Leichterer Zugang zu Schadsoftware, bewusst Krankenhäuser als Ziel

Organisationale Maßnahmen für mehr Sicherheit
- Schulung, ISMS, positive Kultur und Identifikation mit Organisation, spezielle Sicherheitsteams

Menschliche Faktoren bei IT-Risiken in Krankenhäusern

Anstieg des Risikobewusstseins
- Bessere Erkennung von Phishing, starker Anstieg insbesondere nach einem Vorfall

Persönliches Sicherheitsverhalten überträgt sich in den Beruf
- Nutzung persönlicher Endgeräte, offenes Teilen von Daten, absichtliches Fehlverhalten

Hauptziel für Cyberkriminelle
- Arbeitsumfeld führt zu Vorfällen, Hauptfaktor für das Eintreten von Vorfällen

Heterogenität der Mitarbeiter
- Unterschiedliche Offenheit und Kompetenz gegenüber Cybersicherheit, respektvolle und gezielte Kommunikation notwendig

Diskussion

Die erarbeiteten Datensätze liefern eine umfassende Grundlage für die Analyse von Cyber- und Datenschutzvorfällen im Gesundheitswesen. Der Großteil der Vorfälle entfiel auf externes Hacking, insbesondere Ransomware-Angriffe, die auch in den Fokusgruppen als zentrales Risiko identifiziert wurden. Rund ein Viertel der Vorfälle stand im Zusammenhang mit menschlichen Faktoren, die auch ein großes Themencluster während der Fokusgruppen bildeten. Die Kombination aus Fokusgruppen und der Analyse realer Vorfälle half, Wissenslücken zu schließen, IT-Risiken in Krankenhäusern präziser zu verstehen und wachsende Bedrohungen zu erkennen. Als positive Tendenz ist das zunehmende Risikobewusstsein im Zusammenhang mit Phishing hervorzuheben.
Unter aktuellen Risiken wurde häufig die Übertragung des privaten Umgangs mit digitalen Anwendungen und Geräten in den beruflichen Kontext genannt. Potential für weitere Forschung bietet vor allem der Umgang mit externen Dienstleistern und Zulieferern.

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; 11:1196596

[2] Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: A systematic review. Technology and health care : official journal of the European Society for Engineering and Medicine 2016; 24(1):1–9.

[3] Theocharidou M, Lella I. enisa Threat Landscape: Health Sector: (January 2021 to March 2023); 2023 [abgerufen am 13.11.2025]. Verfügbar unter: https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

[4] Ignatovski M. For-profit versus non-profit cybersecurity posture: breach types and locations in healthcare organisations. Health information management : journal of the Health Information Management Association of Australia 2024; 53(3):198–205

[5] Dolezel D, McLeod A. Cyber-Analytics: Identifying Discriminants of Data Breaches. Perspectives in Health Information Management 2019; 16(Summer):1a.

[6] Ronquillo JG, Erik Winterholler J, Cwikla K, Szymanski R, Levy C. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA open 2018; 1(1):15–9.

ATLAS DIGITALE GESUNDHEITSWIRTSCHAFT

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

Gefördert durch das Land Nordrhein-Westfalen