Kurzbericht zum BMG-geförderten Forschungsvorhaben

Vorhabentitel	MedISA – Medical Centre Employee Centered Information Security Awareness
Schlüsselbegriffe	Informationssicherheitsbewusstsein, Nudging, Gesundheitswesen, Awareness-Maßnahmen, Phishing-Simulation
Vorhabendurchführung	Hochschule Bonn-Rhein-Sieg in Kooperation mit Universitätskliniken Aachen, Düsseldorf, Bonn und Frankfurt
Vorhabenleitung	Prof. Dr.-Ing. Luigi Lo Iacono
Autoren	Prof. Dr.-Ing. Luigi Lo Iacono, Dr. David Langer und Dr. Jan Tolsdorf
Vorhabenbeginn	01.12.2021
Vorhabenende	31.12.2024

1. Vorhabenbeschreibung, Vorhabenziele

Die zunehmende Digitalisierung im Gesundheitswesen erhöht die Verwundbarkeit gegenüber Cyberangriffen. Der Gesundheitssektor gehört laut ENISA zu den am häufigsten betroffenen Branchen [1]. Fälle wie der IT-Ausfall am Universitätsklinikum Düsseldorf 2020 oder an der Universitätsmedizin Frankfurt 2023 zeigen, wie stark Cybervorfälle die medizinische Versorgung gefährden können. Trotz technischer und organisatorischer Standards wie dem B3S [2] bleibt der menschliche Faktor eine zentrale Schwachstelle. Fehlendes Informationssicherheitsbewusstsein (Information Security Awareness, ISA) bei Beschäftigten gilt als häufige Ursache für Sicherheitsvorfälle [3].

Obwohl zahlreiche Methoden zur Förderung von ISA existieren, mangelt es im klinischen Alltag an wirksamen, ressourcenschonenden und breit akzeptierten Maßnahmen, die sich nachhaltig integrieren lassen. Bestehende Ansätze werden selten systematisch evaluiert oder erreichen nicht alle Berufsgruppen gleichermaßen. Zwar bot das EU-Horizon-Projekt PANACEA [4] vielversprechende Impulse, dennoch bleibt der Bedarf an evidenzbasierten, alltagstauglichen ISA-Maßnahmen weiterhin hoch.

Vor diesem Hintergrund wurde MedISA konzipiert. Ziel des vom Bundesministerium für Gesundheit geförderten Projekts war es, ein nutzerzentriertes Bündel an ISA-Maßnahmen für den Klinikalltag zu entwickeln, prototypisch umzusetzen und wissenschaftlich zu evaluieren. Die Maßnahmen wurden in enger Zusammenarbeit mit Beschäftigten verschiedener Berufsgruppen entwickelt. Neben klassischen Maßnahmen lag der Fokus auf die Entwicklung und Evaluation von Nudges ist – ein gezielter

Anstoß, der menschliches Verhalten auf vorhersehbare Weise beeinflusst, indem er kognitive Routinen und Entscheidungsgewohnheiten nutzt, ohne dabei Zwang auszuüben [5]. Damit sollte sicheres Verhalten durch verhaltenspsychologische Elemente alltagsnah gefördert, ohne zusätzliche Belastungen zu erzeugen.

2. Durchführung, Methodik

Die Methodik kombinierte qualitative und quantitative Verfahren. Zur methodischen Fundierung wurden gesetzliche Vorgaben, branchenspezifische Standards wie der B3S sowie menschliche Faktoren der Informationssicherheit im Gesundheitswesen analysiert. Ergänzend wurden aktuelle Forschungsansätze zu ISA, Awareness-Methoden, psychometrischen Messinstrumenten sowie das EU-Horizon-Projekt PANACEA aufgearbeitet.

Im Rahmen qualitativer Vorarbeiten wurden sechs Interviews mit Fachpersonen aus medizinischen Einrichtungen und Dienstleistungsunternehmen durchgeführt, um Erfahrungen mit bestehenden ISA-Maßnahmen zu erfassen. Ergänzend fanden vier Workshops mit Beschäftigten aus verschiedenen Berufsgruppen statt, um praxisrelevante Hürden und Anreize im Umgang mit Informationssicherheit zu identifizieren. Darüber hinaus wurden auf Basis von vier weiteren Fokusgruppen mit Personen aus dem ärztlichen Dienst und Pflegedienst konkrete Nudge-Ideen entwickelt sowie in Zusammenarbeit mit einer Stabstelle für Informationssicherheit eine Phishing-Simulation konzipiert. Parallel wurde ein bestehendes psychometrisches ISA-Messinstrument thematisch erweitert, zweisprachig aufbereitet und als Kurzversion zur praktischen Anwendung optimiert.

Zur Evaluation kamen quantitative Verfahren zum Einsatz: Eine Online-Studie mit 487 Personen untersuchte den Einfluss von psychologischen Interventionen auf Sicherheitsmüdigkeit. Zwei Validierungsstudien mit insgesamt 1.779 Teilnehmenden prüften die Qualität des psychometrischen ISA-Messinstruments. Zudem wurden in einer Universitätsklinik zwei groß angelegte Phishing-Simulationen mithilfe experimenteller Designs bei über 7.000 Mitarbeitenden durchgeführt, um die Wirksamkeit verschiedener E-Mail-Gestaltungsmerkmale und Gegenmaßnahmen durch Anti-Phishing-Nudges zu analysieren.

3. Gender Mainstreaming

Im MedISA-Projekt wurde Gendermainstreaming systematisch berücksichtigt. Geschlechteraspekte flossen in Konzeption, Rekrutierung und Analyse ein, qualitative Formate wurden möglichst divers besetzt und Materialien durchgängig geschlechtergerecht gestaltet, um eine inklusive Ansprache und höhere Wirksamkeit der ISA-Maßnahmen zu erreichen.

4. Ergebnisse, Schlussfolgerung, Fortführung

Das Projekt entwickelte ein breites Repertoire an ISA-Maßnahmen mit 56 konkreten Nudge-Ideen, etwa durch sichtbare Führungskräftekommunikation, QR-Codes auf Dienstausweisen, visuelle Erinnerungen und spielerische Wettbewerbe. Eine Phishing-Simulation mit über 7000 Mitarbeitenden

zeigte, dass einfache digitale Anti-Phishing-Nudges wie deutlich gestaltete Warnbanner oder deaktivierte Links das Risiko deutlich senken, Passwörter preiszugeben, während das Extern-Tagging weitestgehend wirkungslos blieb. Ergänzend wurden Erkenntnisse zur Messung von ISA gewonnen, indem mit dem sHAIS-Q ein psychometrisches Instrument entwickelt wurde, das Wissen, Einstellungen und selbst eingeschätztes Verhalten zur Informationssicherheit effizient und bei Bedarf differenziert erfassen kann und zudem technische KPIs identifiziert, die eine objektive Bewertung von ISA ermöglichen.

Die Projektergebnisse wurden über eine zweisprachige Website sowie verschiedene Fachformate einer breiten Fachöffentlichkeit zugänglich gemacht, unter anderem durch Beiträge in relevanten Fachmedien, die Präsentation auf der DMEA 2025 und die Einreichung bei wissenschaftlichen Konferenzen.

Die MedISA-Ergebnisse bieten hohes Transferpotenzial für Praxis, Politik und Forschung: Sie ermöglichen anwendbare, partizipativ entwickelte und evidenzbasiert evaluierte Maßnahmen zur Stärkung der Informationssicherheit im Gesundheitswesen und liefern Impulse für gesetzgeberische Vorhaben im Kontext von NIS-2 und KRITIS sowie für branchenspezifische Sicherheitsstandards wie den B3S. Ein geplantes Start-up soll die nachhaltige Weiterentwicklung wirksamer, praxisnaher und skalierbarer ISA-Maßnahmen sichern.

5. Umsetzung der Ergebnisse durch das BMG

Die Ergebnisse des Projekts leisten einen wertvollen Beitrag zu den laufenden Überlegungen zur Stärkung der Informationssicherheit im Gesundheitswesen. Die gewonnenen Erkenntnisse können in künftige fachliche und strategische Diskussionen zu Themen wie Informationssicherheit, Umsetzung der NIS-2-Richtlinie und branchenspezifische Sicherheitsstandards (B3S) aber auch in den Förderleitfaden zum „Sofortprogramm Cybersicherheit“ einfließen.

6. Verwendete Literatur

[1] European Union Agency for Cybersecurity., *ENISA threat landscape 2023: July 2022 to June 2023.* LU: Publications Office, 2023. Accessed: Jun. 21, 2025. [Online]. Available: https://data.europa.eu/doi/10.2824/782573

[2] Deutsche Krankenhaus Gesellschaft, “Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus,” Oct. 2019. Accessed: Mar. 20, 2022. [Online]. Available: https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf

[3] L. Jaeger, “Information Security Awareness: Literature Review and Integrative Framework,” 2018.

[4] S. Magalini, “Cyberthreats to Hospitals: Panacea, a Toolkit for People-Centric Cybersecurity“,” *J Strateg Innov Sustain Bd*, vol. 16, no. 3, Art. Nr. 3, Aug. 2021, doi: 10.33423/jsis.v16i3.4449.

[5] P. G. Hansen, “The Definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove?“,” *Eur J Risk Regul Bd*, vol. 7, no. 1, pp. 155-174, 2016, doi: 10.1017/S1867299X00005468.

Gefördert durch:

Bundesministerium
für Gesundheit

aufgrund eines Beschlusses
des Deutschen Bundestages