# Abschlussbericht zum Projekt

## MedISA

### Medical Centre Employee Centered Information Security Awareness


**Zuwendungsempfänger**
Hochschule Bonn-Rhein-Sieg
53754 Sankt Augustin



**Förderkennzeichen**
ZMI1-2521FSB801



**Projektleitung**
Prof. Dr.-Ing. Luigi Lo Iacono
Gruppe für Daten und Anwendungssicherheit
Institut für Cyber Security & Privacy
Fachbereich Informatik
Grantham-Allee 20
53757 Sankt Augustin

**Projektmitarbeiter**
Dr. Jan Tolsdorf
Dr. David Langer



**Projektlaufzeit**
01.12.2021 - 31.12.2024

**Fördersumme**
450.000 €

**Erstellungsdatum**
30. Juni 2025



Gefördert durch:

Bundesministerium für Gesundheit

aufgrund eines Beschlusses des Deutschen Bundestages


Hochschule Bonn-Rhein-Sieg
University of Applied Sciences

/DAS>

# Inhaltsverzeichnis

# Tabellen- und Abbildungsverzeichnis

# 1 Zusammenfassung

Das Forschungsprojekt MedISA (Medical Centre Employee Centered Information Security Awareness) zielte darauf, alltagstaugliche Maßnahmen zur Förderung des Informationssicherheitsbewusstseins (Information Security Awareness, ISA) in medizinischen Versorgungseinrichtungen zu entwickeln. Angesichts wachsender Cyberbedrohungen stand dabei der Mensch als zentrale Schwachstelle im Fokus, weshalb praxisnahe Lösungen zur Stärkung der Handlungskompetenz und aktiven Einbindung der Beschäftigten erarbeitet und evaluiert wurden.

Zwar existieren zahlreiche Methoden zur Steigerung von ISA, doch fehlt es insbesondere im Gesundheitswesen an praxistauglichen, evidenzbasierten und ressourcenschonenden Ansätzen, die nachhaltig wirken und die verschiedene Personalgruppen einbeziehen. Zudem fehlt es an systematischen Wirksamkeitsnachweisen.

Das Ziel des MedISA-Projekts war, ISA-Maßnahmen und Materialien mit einem besonderen Fokus auf sogenannte Nudges, also psychologische Verhaltensanreize, zu entwickeln, die das Personal dazu bewegen sollen, sicherheitsbewusste Entscheidungen zu treffen, ohne dabei auf Zwang oder komplexe technische Schutzmaßnahmen zurückzugreifen.

Die Maßnahmen wurden partizipativ mit Beschäftigen aus dem ärztlichen Dienst, Pflegedienst, Verwaltung, IT und Stabstellen der Informationssicherheit an vier Universitätskliniken sowie in verwandten Dienstleistungsunternehmen entwickelt. Mithilfe qualitativer und quantitativer Methoden, darunter Workshops, Fokusgruppen, Experten- und Expertinnen-interviews, Experimente und Umfragen, wurden sie praxisnah unter den realen Bedingungen des Krankenhausalltags entwickelt und erprobt.

Das Projekt entwickelte ein breites Repertoire an ISA-Maßnahmen mit 56 konkreten Nudges, etwa durch sichtbare Führungskräftekommunikation, QR-Codes auf Dienstausweisen, visuelle Erinnerungen und spielerische Wettbewerbe. Eine Phishing-Simulation mit über 7.000 Mitarbeitenden zeigte, dass einfache digitale Anti-Phishing Nudges wie deutliche Warnbanner oder deaktivierte Links das Risiko deutlich senken, Passwörter preiszugeben. Ergänzend wurde mit dem sHAIS-Q ein psychometrisches Messinstrument geschaffen, das Wissen, Einstellungen und Verhalten zur Informationssicherheit effizient und bei Bedarf auf Basis einer dedizierten Erweiterung differenzierter erfasst.

Die Ergebnisse zeigen, dass Informationssicherheit besonders wirksam ist, wenn Maßnahmen praxisnah, zielgruppenspezifisch und gemeinsam mit dem Klinikpersonal gestaltet werden. MedISA verbindet wissenschaftliche Erkenntnisse mit praktischen Anforderungen und stellt frei verfügbare Werkzeuge bereit, die als übertragbares Modell zur Stärkung der Sicherheitskultur im Gesundheitswesen dienen.

# 2 Einleitung

Die zunehmende Digitalisierung im Gesundheitswesen birgt neben enormen Chancen auch erhebliche Risiken. Einrichtungen der medizinischen Versorgung geraten dabei zunehmend ins Visier von Cyberangriffen, die nicht nur wirtschaftlichen Schaden verursachen, sondern auch die Verfügbarkeit und Integrität kritischer Infrastrukturen gefährden können. Laut dem Lagebericht 2024 des Bundesamts für Sicherheit in der Informationstechnik (BSI) bleibt die Bedrohungslage im Cyberraum angespannt, da Kriminelle immer professioneller agieren, neue Schwachstellen gezielt ausnutzen und zunehmend vielfältige Angriffsformen auf Unternehmen, Behörden und die Gesellschaft anwenden [1]. Laut einem Bericht der Agentur der Europäischen Union für Cybersicherheit (ENISA) gehört der Gesundheitssektor 2023 zu den drei Branchen, die am häufigsten Ziel von Cyberangriffen sind [2]. Fälle wie der temporäre Ausfall des Universitätsklinikums Düsseldorf im Jahr 2020 [3] oder der Universitätsmedizin Frankfurt im Jahr 2023 [4] unterstreichen die potenzielle Bedrohung für die medizinische Versorgung.
Technische und organisatorische Schutzmaßnahmen wie sie u. a. im Branchenspezifischen Sicherheitsstandard für Krankenhäuser (B3S) vorgeschrieben sind, sind wichtige Säulen der IT-Sicherheit. Dennoch bleibt der „Faktor Mensch" ein zentraler Schwachpunkt. Das mangelnde Bewusstsein für Informationssicherheit (Information Security Awareness, ISA) bei Mitarbeiterinnen und Mitarbeitern wird in der Praxis als kritischer Risikofaktor identifiziert. Fehlendes Wissen über potenzielle Gefahren, eine geringe Risikowahrnehmung sowie unsachgemäßer Umgang mit IT-Systemen führen häufig zu Sicherheitsverstößen. Der B3S mit der Anforderung ANFMN70 – der ISO 27001 A.7.2.2 folgend – fordert daher verpflichtende ISA-Schulungen für alle Beschäftigten mindestens alle zwei Jahre (vgl. [5]).
Der wissenschaftliche Diskurs bestätigt, dass Informationssicherheitsbewusstsein ein zentraler Faktor für das sicherheitskonforme Verhalten von Beschäftigten ist (vgl. z. B. [6], [7], [8], [9]). ISA umfasst dabei nicht nur die reine Wissensvermittlung, sondern einen längerfristigen Prozess zur Etablierung sicherheitsförderlicher Einstellungen, Werte und Gewohnheiten (vgl. [10], [11]). Verschiedene Studien belegen, dass das Verhalten von Mitarbeitern und Mitarbeiterinnen im sicheren Umgang mit Informationssystemen sowie die Einhaltung von Informationssicherheitsvorgaben von zahlreichen Einflussfaktoren bestimmt werden [7], [12].
Die Analyse des aktuellen Stands der Wissenschaft zeigt allerdings, dass zwar eine Vielzahl an Methoden zur Steigerung des Informationssicherheitsbewusstseins existiert, deren Wirksamkeit jedoch oft nur punktuell belegt ist, nicht systematisch verglichen wurde oder sich nicht ohne Weiteres auf größere Organisationen im Gesundheitswesen übertragen lässt. Zwar widmete sich das EU-Horizon-2020-Projekt PANACEA [13], [14],

[15] u.a. explizit der Entwicklung von Awareness- und Nudging-Maßnahmen im Gesundheitsbereich, hat jedoch kein umfassendes Repertoire und auch kein systematische Evaluation der Prototypen im Feld vorgelegt. Im Gesundheitssektor mangelt es daher weiterhin an praxistauglichen, evidenzbasierten und zugleich ressourcenschonenden Ansätzen, die nachhaltig Wirkung entfalten und heterogene Personalgruppen in medizinischen Versorgungseinrichtungen einbeziehen.
Vor diesem Hintergrund wurde das Projekt MedISA – Medical Centre Employee Centered Information Security Awareness – konzipiert, das vom Bundesministerium für Gesundheit (BMG) gefördert und von der Hochschule Bonn-Rhein-Sieg (H-BRS) in Kooperation mit den Universitätskliniken Aachen (UKAC), Düsseldorf (UKD), Bonn (UKB) und Frankfurt (UKF) umgesetzt wurde. Ziel war es, praxisnahe, akzeptierte und wirksame Maßnahmen zur Stärkung der ISA in medizinischen Versorgungseinrichtungen zu entwickeln, die sich nachhaltig in den Arbeitsalltag integrieren lassen.
Das übergeordnete Ziel des MedISA-Projekts war die Entwicklung, prototypische Umsetzung und wissenschaftliche Evaluation eines nutzerzentrierten Bündels an Maßnahmen zur Förderung des Informationssicherheitsbewusstseins. Diese Maßnahmen sollten passgenau auf verschiedene Zielgruppen wie Pflegedienst, den ärztlichen Dienst sowie auf weitere Personalgruppen zugeschnitten sein, gleichzeitig praktikabel, wirtschaftlich tragfähig, nachhaltig wirksam und auf andere Einrichtungen übertragbar sein. Im Zentrum stand dabei die kontinuierliche Sensibilisierung im Arbeitsalltag, unter anderem durch den Einsatz von Nudging-Ansätzen. Ein Nudge ist eine Form der Verhaltensintervention, bei der versucht wird, das Verhalten von Menschen gezielt zu beeinflussen, ohne Zwang oder ökonomische Anreize einzusetzen (ein sogenannter „Stups“ in eine gewünschte Richtung) [16].

Der Aufbau des Projekts gliederte sich in fünf aufeinander aufbauende Arbeitspakete (AP):

- **AP1:** Methodische Vorarbeiten und systematische Analyse bestehender ISA-Maßnahmen.
- **AP2**: Untersuchung bisheriger Awareness-Initiativen in den Partnerkliniken mittels Metastudien und Interviews.
- **AP3**: Partizipative Entwicklung innovativer ISA-Maßnahmen und Materialien mit den relevanten Nutzergruppen.
- **AP4**: Evaluation der entwickelten Prototypen unter realitätsnahen Bedingungen.
- **AP5**: Projektmanagement, Öffentlichkeitsarbeit und Wissenstransfer.

Die in MedISA gewonnenen Erkenntnisse wurden in einem zielgruppenspezifischen Maßnahmenkatalog dokumentiert und stehen über eine projektbegleitende Website

(https://medisa-projekt.de/catalogue/) zur weiteren Nutzung bereit. So trägt MedISA durch seine Ergebnisse nachhaltig zur Verbesserung der Informationssicherheit in der medizinischen Versorgung bei.

# 3 Erhebungs- und Auswertungsmethodik

Zur Erreichung der dargestellten Projektziele in Tabelle 1 kamen verschiedene qualitative und quantitative Methoden der Datenerhebung und -auswertung zum Einsatz. Die Datenerhebung erfolgte unter anderem durch Workshops, Interviews, Online-Umfragen und Phishing-Simulationen. Zur Auswertung wurden qualitative Inhaltsanalysen, thematische Analysen, psychometrische Validierungen sowie weitere statistische Verfahren eingesetzt, um fundierte Erkenntnisse über ISA, wirksame ISA-Maßnahmen und deren Einflussfaktoren zu gewinnen.

**Tabelle 1:** Zeile, Teilziele sowie die Indikatoren zur Messung der Zielerreichung

| Ziele (Arbeitspakete) | Teilziele | Indikatoren zur Messung der Zielerreichung |
|---|---|---|
| **AP1: Methodische Vorarbeiten: Aktualisierter Forschungsstand (Literaturüberblick) und eine Systematisierung bestehender ISA-Methoden.** | Z1: Erhebung des aktuellen Forschungsstand | Systematischer Literaturüberblick abgeschlossen und dokumentiert. |
| **AP2: Analyse ergriffener Awareness-Maßnahmen: Untersuchung bisheriger Maßnahmen in Kliniken und deren Akzeptanz/Wirkung sowie Identifikation relevanter Anwendungsfälle.** | Z2: Erfahrungsgewinn aus bereits angebotenen ISA-Materialien und durchgeführten ISA-Maßnahmen (Literatur, Interviews, Studien). | Anzahl semi-strukturierter Einzelinterviews mit Expertinnen und Experten für Informationssicherheit in medizinischen Einrichtungen sowie Ergebnisse der Literaturrecherche zu relevanten ISA-Maßnahmen. |
| | Z3: Anforderungserhebung und Identifikation von Hürden/Anreizen. | Anzahl Workshops und Workshopteilnehmer sowie Ergebnisse der Literaturrecherche zu den Hürden und Anreize in medizinischen Versorgungseinrichtungen. |
| **AP3: Partizipative Entwicklung von MedISA-Maßnahmen: Entwicklung von MedISA-Prototypen mit Zielgruppen, inkl. Nudging-Ansätzen sowie MedISA-Maßnahmenkatalog.** | Z4: Partizipatives Design von ISA-Maßnahmen mit Zielgruppen. | Anzahl Workshops und Anzahl teilnehmender Personen sowie Ergebnisse Literaturrecherche zu partizipativem Design |
| | Z5: Entwicklung von prototypischen ISA-Maßnahmen und ISA-Materialien | Anzahl an ISA-Maßnahmen und ISA-Materialien sowie Erstellung und Einbindung in einen online verfügbaren Maßnahmenkatalog. |
| | Z6: Entwicklung neuartiger Nudges zur minimalinvasiven Integration in den Arbeitsalltag. | Anzahl von Workshops und Anzahl teilnehmender Personen sowie Anzahl von minimalinvasiven Nudges |
| **AP4: Evaluation der MedISA-Maßnahmen: Bewertung der Maßnahmen hinsichtlich Wirksamkeit, Praktikabilität und Skalierbarkeit.** | Z7: Evaluation der MedISA-Prototypen durch Nutzerstudien. | Anzahl teilnehmender Personen aus Access Panels und Kliniken, einschließlich einer Unterscheidung zwischen medizinischem und nichtmedizinischem Personal, Durchführbarkeit der MedISA-Prototypen, Usability der ISA-Maßnahmen, kausale Wirksamkeit der entwickelten ISA-Maßnahmen und Nudges zur Steigerung der Informationssicherheit. |

| | | |
|---|---|---|
| **AP5: Projektmanagement, Öffentlichkeitsarbeit und Transfer: Sicherstellung der Kommunikation, Transfer und Nachhaltigkeit der Projektergebnisse.** | Z8: Alle benötigten Dokumente und Verträge sind vorhanden. | Vollständige Bereitstellung der Projektbasisdokumente (z. B. Verträge, Webseite) |
| | Z9: Dissemination der Projektergebnisse | Anzahl veröffentlichter zielgruppenspezifischer Leitfäden, Maßnahmen sowie Messinstrumente via Website, Medien und Konferenzen; Anzahl eingereichter/akzeptierter wissenschaftlicher und praxisorientierter Publikationen. |

**Im Rahmen von AP1** und **Z1** wurde die gesetzlichen und normativen Grundlagen der Informationssicherheit in Krankenhäusern als Basis für die weitere Literaturrecherche ermittelt, darunter das BSI-Gesetz, die IT-Sicherheitsgesetze und die BSI-Kritisverordnung [17]. Im Fokus standen die Pflichten medizinischer Einrichtungen als kritische Infrastruktur KRITIS und Nicht-KRITIS sowie branchenspezifische Sicherheitsstandards (B3S, [5]), zentrale Schutzziele, relevante Stakeholder und der Einfluss menschlicher Faktoren. Darauf aufbauend wurde der aktuelle Forschungsstand zu Informationssicherheits-Awareness (ISA) sowie ISA-Vermittlungsmethoden analysiert, insbesondere das EU-Horizon-Projekt „PANACEA" mit seinem Toolkit für Cybersicherheit und Nudging-Interventionen [13], [14]. Zudem wurde die Literatur um Ansätze zur psychometrischen Messung von ISA erweitert.

**Im Rahmen von AP2** wurden für **Z2** sechs (n = 6) semi-strukturierte Einzelinterviews aus fünf medizinischen Versorgungseinrichtungen und verwandte Dienstleistungsunternehmen durchgeführt, um Erfahrungswerte mit bestehenden ISA-Materialien und -Maßnahmen in medizinischen Versorgungseinrichtungen zu erheben. Befragt wurden Expertinnen und Experten aus verschiedenen Funktionsbereichen mit Aufgaben in der Informationssicherheit, darunter ISBs, Mitglieder von ISMS-Teams, IT- und Datenschutzberatung sowie Leitungen aus Qualitäts- und Projektmanagement. Thematisiert wurden u.a. Erfahrungen mit Informationssicherheit und Angriffen, der Einfluss auf Patientinnen und Patienten, der Faktor Mensch, Art, Umfang und Qualität von ISA-Maßnahmen, Zielgruppenspezifik, Wirksamkeit, Kosten sowie Optimierungspotenziale. Die Auswertung erfolgte mittels Thematic Analysis.

**Im Rahmen von AP2** wurden für **Z3** zur Identifikation von Anreizen und Hürden vier Workshops bei einem assoziierten Partner mit insgesamt n = 13 Personen mit unterschiedlicher Personalgruppen durchgeführt. befragten Personalgruppen lassen sich zusammenfassen als medizinisches Fachpersonal (z. B. Ärztinnen/Ärzte, Assistenzarzt, Krankenschwester, Oralchirurg, Optometrist), administrative und organisatorische Fachkräfte (z. B. Abteilungsleitung, Patientenmanagement, Sachbearbeitung),

technisches Personal (z. B. Ingenieur, Sicherheitsingenieur) sowie wissenschaftliches Personal. Die Auswertung erfolgte mittels qualitativer Inhaltsanalyse.

**Im Rahmen von AP3** wurden für **Z4** partizipativ mit relevanten Zielgruppen in insgesamt drei Workshops mit n = 19 Personen an zwei Universitätskliniken ISA-Maßnahmen und erste ISA-Maßnahmen und Materialien entwickelt: Bei einem assoziierten Partner fand eine Fokusgruppe mit n = 10 Teilnehmenden aus der IT-Abteilung, dem CISO-Bereich und den ISBs der Uniklinik Düsseldorf statt, um mögliche Key Performance Indicators (KPIs) zur Messung von ISA zu identifizieren. In einer weiteren Klinik wurde in einem Workshop mit dem Personalrat und der Stabsstelle Informationssicherheit (n = 6) die Zustimmung für eine zielgruppenspezifische Phishing-Simulation eingeholt und geklärt, welche Maßnahmen unter Berücksichtigung begrenzter Datenzugänge realisierbar sind. Ergänzend fand ein weiterer Workshop mit der Stabsstelle Informationssicherheit zur Entwicklung konkreter Untersuchungsdesigns für die geplante Phishing-Simulation statt (n = 3). Zusätzlich wurde auf Forschungsergebnisse des EU-Projekts „PANACEA“ mit seinem Toolkit für Cybersicherheit und Nudging-Interventionen zurückgegriffen, das ein partizipatives Framework zur Entwicklung von Nudges beinhaltet [18].

**Im Rahmen von AP3** wurden für **Z5** ISA-Maßnahmen und Messinstrumente entwickelt. Ein etabliertes psychometrisches Messinstrument wurde thematisch ergänzt, zweisprachig (Deutsch/Englisch) aufbereitet und um eine Kurzversion erweitert. Solche Instrumente dienen nicht nur der Messung von ISA, sondern können – durch ihre aktivierende Wirkung auch selbst als Maßnahme verstanden werden. Für die experimentelle Erhebung wurde ein Studiendesign entworfen, das die kausale Wirkung einzelner Merkmale in einer Phishing-Simulation untersuchen kann (experimenteller Plackett-Burman [19]- und Between-Subject-Versuchsplan). Zudem wurde auf acht Schulungsvideos aus dem EU-Horizon-Projekt PANACEA zurückgegriffen [20], [21], indem durch eine Kooperation mit den Projektpartnern und -partnerinnen der Erhalt der Nutzungsrechte erfolgte (Lizenzhalter: RINA Tech UK Ltd). Darüber hinaus wurde die digitale Infrastruktur des Maßnahmenkatalogs entwickelt und fortlaufend ergänzt.

**Im Rahmen von AP3** wurde für **Z6** in (1) zwei Workshops mit der Stabsstelle Informationssicherheit (jeweils n = 3) zunächst gefährliche Merkmale von Phishing-Mails identifiziert und anschließend die technische Umsetzbarkeit von 11 potenziellen Nudges als Gegenmaßnahmen in einer Phishing-Simulation identifiziert. (2) Des Weiteren fanden an einer weiteren Universitätsklinik insgesamt vier Fokusgruppen auf Grundlage der AIDE- und MINDSPACE-Ansätze aus dem PANACEA-Toolkit statt: zwei Teil-I-Fokusgruppen getrennt nach Personalgruppen mit Teilnehmenden aus dem ärztlichen Dienst (n = 3) und dem Pflegedienst (n = 5), in denen auf Basis zuvor quantitativ eingegrenzter Themenbereiche sicherheitskritische Arbeitsabläufe identifiziert wurden.

Darauf aufbauend folgten zwei Teil-II-Fokusgruppen, erneut getrennt nach Personalgruppen, mit Teilnehmenden aus dem ärztlichen Dienst (n = 4) und dem Pflegedienst (n = 3), in denen gemeinsam mögliche Nudges zur Förderung sicherheitsbewussten Verhaltens entwickelt wurden. Als Ergebnis wurden 56 praktikable Nudging-Ideen entwickelt, basierend auf den Workshop-Erkenntnissen und der konzeptionellen Weiterentwicklung durch das MedISA-Forscherteam. (3) Darüber hinaus wurden einer anderen Studie anreizbasierten und motivationsbasierten Nudges im MedISA-Forschungsteam entwickelt, um den Einfluss auf Sicherheitsmüdigkeit sowie Passwortstärke zu untersuchen.

**Im Rahmen von AP4** stand bei **Z7** die Evaluation der entwickelten und identifizierten ISA-Maßnahmen im Fokus. Dabei wurden drei zentrale Untersuchungen durchgeführt: (1) Eine Online-Studie mit n = 487 Teilnehmenden aus einem Access-Panel untersuchte den Zusammenhang zwischen anreiz- und motivationsbasierten Nudges und deren Einfluss auf Sicherheitsmüdigkeit. (2) Das psychometrische ISA-Messinstrument wurde in mehreren Validierungsphasen mit insgesamt N = 2.948 Personen getestet: zunächst in einer Pilotstudie mit n = 1.182 Personen aus einem Access-Panel, danach im Praxistest mit n = 1.187 Personen in zwei Universitätskliniken. Nach Überarbeitung aufgrund unzureichender wissenschaftlicher Güte wurde es in einer dritten Universitätsklinik mit n = 579 Personen erfolgreich validiert und zeigte dabei ausgezeichnete psychometrische Eigenschaften, eine effiziente Durchführung sowie klare Zusammenhänge zu relevanten Hürden und Anreizen im Bereich ISA. (3) Zudem wurden zwei erfolgreiche Phishing-Kampagnen mit insgesamt N = 7.044 Personen in einer Universitätsklinik durchgeführt, um zu analysieren, welche Phishing-Merkmale – differenziert nach Personalgruppen – kausal zur Preisgabe von Passwörtern verleiten und mit welchen Nudging-Maßnahmen diesen wirksam begegnet werden kann.

**Im Rahmen von AP5** und **Z8** sowie **Z9** lag der Fokus auf Bereitstellung der Projektbasisdokumente (z. B. Verträge, Webseite) sowie der wissenschaftlichen Verwertung, Öffentlichkeitsarbeit und Dissemination der Projektergebnisse. Dazu gehörten die Erstellung der Meilensteinberichte 1 und 2 sowie der Zwischenberichte 2022 und 2023. Die Projektinhalte wurden über eine zweisprachige MedISA-Webseite, Vorlagen und Präsentationen für Partnerinstitutionen sowie gezielte Öffentlichkeitsarbeit verbreitet. Fachbeiträge in renommierten Medien wie der Ärzte-Zeitung, Krankenhaus Technik+Management und Tagesspiegel Background vermittelten zentrale Erkenntnisse einem breiteren Publikum. Darüber hinaus wurden wissenschaftliche Beiträge aufbereitet und bei Konferenzen eingereicht, u. a. zur Wirkung von Nudging auf Sicherheitsmüdigkeit, zur Wirkung von Anti-Phishing-Nudges sowie die psychometrische Messung von Informationssicherheitsbewusstsein. Ein Konferenzbeitrag wurde erfolgreich auf der DMEA 2025 präsentiert. Schließlich wurden 67 Nudging-Maßnahmen als auch

psychometrische Messinstrumente und verhaltensbasierte Key Performance Indikatoren auf der Projektseite im Maßnahmenkatalog veröffentlicht.

# 4 Durchführung, Arbeits- und Zeitplan

**Tabelle 2:** Arbeits- und Zeitplan einschließlich Meilensteine

| **Laufzeit →** | 1. Jahr | | | | 2. Jahr | | | | 3. Jahr | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Arbeitspaket (AP) ↓** | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| AP1: Methodische Vorarbeiten (Z1) | **MS1** | | | | | | | | | | | |
| AP2: Analyse ergriffener Awareness-Maßnahmen (Z2, Z3) | | | **Plan MS2** | | | | **MS2** | | | | | |
| AP3: Partizipative Entwicklung von MedISA-Maßnahmen (Z4, Z5, Z6) | | | | | | | **Plan MS3** | | | | | **MS3** |
| AP4: Evaluation der MedISA-Maßnahmen (Z7) | | | | | | | | | | **Plan MS4** | | **MS4** |
| AP5: Projektmanagement, Öffentlichkeitsarbeit und Transfer (Z8) | | | | | | | | | | | | **MS5** |

In Tabelle 2 ist der Überblick der Arbeitspakte und Meilensteine im Gantt-Diagramm zu sehen. Zu Beginn des Projekts wurde in **AP1 (Methodische Vorarbeiten)** das Teilziel Z1 und MS1 planmäßig im ersten Jahr erreicht. Die methodischen Grundlagen, insbesondere durch Literaturrecherche konnten wie vorgesehen umgesetzt werden. Die

Literaturarbeit wurde im Projektverlauf kontinuierlich fortgeführt und thematisch erweitert, etwa um psychometrische Messinstrumente.

**AP2 (Analyse ergriffener Awareness-Maßnahmen)** sollte planmäßig im dritten Quartal des ersten Projektjahres abgeschlossen sein. Es kam jedoch zu Verzögerungen bei der Umsetzung der Teilziele Z2 und Z3, die insbesondere Einzelinterviews sowie die Durchführung von Fokusgruppen umfassten. Die ursprünglich geplante Anzahl an Interviews und Fokusgruppen konnte nicht vollständig realisiert werden. Dennoch gelang es, durch Rückgriff auf die Ergebnisse des EU-Horizon-2020-Projekts „Panacea" inhaltliche Lücken zu schließen. Auf diese Weise konnte der Meilenstein MS2 im dritten Quartal des zweiten Projektjahres vollständig erreicht werden.

Der Abschluss von **AP3 (Partizipative Entwicklung von MedISA-Maßnahmen)** war für Q3 des 2. Projektjahres vorgesehen. Die Ziele von AP3 und MS3 konnten nach anfänglichen Verzögerungen noch rechtzeitig zum Projektende vollständig erreicht werden: In mehreren Workshops mit IT-Personal, ärztlichem und pflegerischem Personal sowie Stabsstellen wurden gemeinsam ISA-Maßnahmen und Nudging-Ansätze partizipativ entwickelt, ergänzt durch experimentelle Designs, Entwicklung psychometrischer Messinstrumente und Rückgriff auf das EU-Projekt „PANACEA" [13].

In **AP4 (Evaluation)**, das für das zweite Quartal im dritten Projektjahr vorgesehen war, konnte die geplante umfassende Bewertung der entwickelten ISA-Maßnahmen fokussiert umgesetzt werden. Eine Einschränkung bestand jedoch darin, dass die im Rahmen der Fokusgruppen entwickelten Nudging-Ideen aus AP3/Z6 erst gegen Ende der Projektlaufzeit finalisiert wurden und daher nicht mehr in eine Wirksamkeitsbewertung überführt werden konnten. Auch die ursprünglich geplante Untersuchung der Langzeitwirkung von E-Mail-Nudges im Rahmen einer dritten Phishing-Simulationskampagne an einer Universitätsklinik aus AP3/Z4 konnte aus Zeitgründen nicht mehr realisiert werden. Darüber hinaus scheiterte die Evaluation der PANACEA-Schulungsvideos, da Projektpartner kurzfristig absprangen oder die Umsetzung des vorgesehenen Forschungsdesigns seitens der beteiligten Universitätsklinik nicht sachgerecht erfolgte, wodurch die gewonnenen Daten nicht verwertbar waren. Das zusätzlich eingesetzte psychometrische Messinstrument, das ursprünglich nicht vorgesehen war, hat jedoch wesentlich dazu beigetragen, die Evaluation von MedISA trotz dieser Einschränkungen zu erweitern und zu vertiefen.

**AP5 (Projektmanagement, Öffentlichkeitsarbeit und Transfer)** lief kontinuierlich über die gesamte Projektlaufzeit und wurde ohne schwerwiegende Abweichungen durchgeführt. Die Koordination von Projektaktivitäten, der Aufbau der MedISA-Webseite zur Verbreitung von Ergebnissen und die Dissemination und Feedbackgewinnung zu den Projektergebnissen über (wissenschaftliche) Veröffentlichungen erfolgten planmäßig.

**Aufgetretene Probleme und Gegenmaßnahmen**

Im Verlauf des Projekts traten verschiedene strukturelle und operative Probleme auf, die sich erheblich auf die Zielerreichung auswirkten:

Das gravierendste Problem stellte der anhaltende **Personalmangel** dar. Über weite Strecken des Projekts war lediglich eine von zwei vorgesehenen Stellen besetzt. Trotz intensiver Rekrutierungsbemühungen blieb die zweite Stelle zunächst vakant. Erst im April 2023 gelang es, diese zu besetzen. Allerdings schied ein hochqualifizierte Projektmitarbeiter bereits im Februar 2024 wieder aus. Angesichts der kurzen verbleibenden Projektlaufzeit war eine erneute Nachbesetzung von Beginn an unrealistisch. Zusätzlich wurde die Arbeitsfähigkeit weiter durch Elternzeit eingeschränkt.

Ein weiteres zentrales Problem war die **erschwerte Rekrutierung der relevanten Zielgruppen**, insbesondere des ärztlichen und pflegerischen Personals. Trotz der aktiven Unterstützung durch Klinikvorstände und Stabsstellen für Informationssicherheit gelang es nur mit erheblichem Aufwand, relevante Personen für Workshops und Fokusgruppen zu gewinnen. Der Zugang zu diesen Personalgruppen erwies sich als deutlich schwieriger als erwartet, was sowohl die Planung als auch die Umsetzung verschiedener Projektbausteine erheblich verzögerte.

**Streiks** an mehreren Universitätskliniken führten darüber hinaus zu mehrfachen Unterbrechungen geplanter Abstimmungsprozesse und verhinderten zeitweise die Durchführung von Studien. Die Zusammenarbeit mit verschiedenen Partnerkliniken musste in dieser Phase stark reduziert oder ganz ausgesetzt werden.

Zusätzlich kam es zu **zwei gravierenden Vorfällen** in unterschiedlichen Einrichtungen: Zum einen **verlor** das Projektteam eine **zentrale Ansprechpartnerin** in einer Partnerklinik, was die Durchführung geplanter Maßnahmen erheblich verzögerte, und eine aufwendige Neustrukturierung erforderte. Zum anderen führte ein **schwerer Sicherheitsvorfall** in einer weiteren Klinik dazu, dass die geplante Durchführung mehrerer Studien vollständig zum Erliegen kam und erst nach langwierigen Wiederanbahnungen mit Verzögerung fortgesetzt werden konnte.

Darüber hinaus wurde das Projekt durch **fehlende Rückmeldungen** aufgrund eingeschränkter personeller und organisatorischer Ressourcen bei den assoziierten Partnern belastet. Viele Einrichtungen konnten sich aufgrund interner Belastungen oder fehlender Kapazitäten nicht aktiv einbringen. In Einzelfällen wurde eine zuvor zugesicherte Kooperation sogar vollständig zurückgezogen.

Ein strukturelles Hindernis stellten außerdem die **langwierigen internen Abstimmungs- und Genehmigungsprozesse** innerhalb der Kliniken dar. Diese führten wiederholt zu Verzögerungen bei der Planung und Umsetzung von Workshops,

Fokusgruppen der Durchführung von Studien und der praktischen Implementierung geplanter Maßnahmen.
Zur Abmilderung dieser Problemlagen ergriff das Projektteam verschiedene Gegenmaßnahmen. So wurden neue Partnerschaften mit weiteren Kliniken aufgebaut und bestehende Studienprotokolle angepasst. Darüber hinaus griff das Team auf fundierte Erkenntnisse und methodische Vorlagen aus dem EU-Projekt „PANACEA“ zurück. Für die Umsetzung der geplanten Workshops wurde zudem ein externer Forschungsdienstleister eingeplant, um personelle Engpässe und fehlende fachliche Kapazitäten gezielt zu kompensieren. Diese Maßnahmen trugen dazu bei, die Projektziele trotz erheblicher Widrigkeiten weitgehend abzusichern und eine tragfähige Grundlage für mögliche Folgeprojekte zu schaffen.

# 5 Ergebnisse

## Qualitative Ergebnisse aus den Experten- und Expertinnen-Interviews zu ISA-Materialien und durchgeführten ISA-Maßnahmen

Die Interviewstudie basiert auf sechs ausführlichen Gesprächen mit Expertinnen und Experten für Informationssicherheit aus fünf verschiedenen medizinischen Versorgungseinrichtungen sowie zugehörigen Dienstleistungsunternehmen. Von den befragten Personen waren vier Männer und zwei Frauen im Alter zwischen 35 und 64 Jahren. Vier von ihnen arbeiteten direkt in medizinischen Einrichtungen, während zwei als externe Beraterinnen und Berater mit langjähriger Erfahrung in den Bereichen IT, Datenschutz sowie Qualitäts- und Patientensicherheitsmanagement tätig waren. Alle Interviewpartnerinnen und Interviewpartner waren entweder als Informationssicherheitsbeauftragte, in leitenden Positionen innerhalb von Stabsstellen für Informationssicherheit oder im Management von Informationssicherheitsmanagementsystemen (ISMS) tätig. Die beruflichen Hintergründe reichten von der Informatik und Wirtschaftsinformatik über Gesundheitswissenschaften und Gesundheitsökonomie bis hin zu Erfahrungen in der Automobil-, Rüstungs-, Pharma- und Versicherungsbranche.
Die Ergebnisse der Studie in Tabelle 3 verdeutlichen, dass Informationssicherheit in medizinischen Einrichtungen als besonders kritisch eingestuft wird, da sicherheitsrelevante Vorfälle unmittelbare Auswirkungen auf die Gesundheit und das Leben von Patientinnen und Patienten haben können. Zu den größten Herausforderungen zählen technologische Risiken infolge zunehmender Automatisierung und Vernetzung, eine häufig unzureichende Umsetzung von Patchmanagement sowie strukturelle Komplexität, insbesondere in Universitätskliniken mit ihrer Dreifachverantwortung für Versorgung, Lehre und Forschung. Hinzu kommt ein ausgeprägter Personalmangel, der sowohl das medizinisch-pflegerische Personal als auch IT-Fachkräfte betrifft und die Umsetzung eines ISMS deutlich erschwert. Fünf der sechs interviewten Expertinnen und Experten identifizierten Phishing-Angriffe als zentrales Risiko. Der Faktor Mensch wurde dabei ambivalent betrachtet – einerseits als Schwachstelle durch Nachlässigkeit oder fehlende Sensibilität, andererseits als potenzielle Ressource in Form einer „menschlichen Firewall", sofern geeignete Schulungsmaßnahmen erfolgen. ISA-Maßnahmen konzentrieren sich aktuell in der Regel auf zwei bis drei Personalgruppen, insbesondere IT-Personal, Pflegekräfte oder Verwaltungsangestellte, ohne diese differenziert anzusprechen. Wesentliche Herausforderungen sind ein hoher Zeitdruck, eine mangelhafte Unterstützung durch die Leitungsebene und unpassende, oft zu generische Schulungsmaterialien. Während moderne Vermittlungsformen wie Online-

Trainings und interaktive Schulungen als vielversprechend eingeschätzt werden, gelten klassische Methoden wie Poster oder Handzettel als wenig wirksam. Eine systematische Evaluation der ISA-Maßnahmen findet bislang nicht statt, wurde jedoch von mehreren Expertinnen und Experten als dringend notwendig bezeichnet.

**Tabelle 3:** Schlüsselthemen und Befunde aus sechs Experten- und Expertinnen-Interviews zur Informationssicherheit im Gesundheitswesen

| Kategorie | Ergebnisse |
|---|---|
| Kritikalität & Komplexität | Die Informationssicherheit im Gesundheitswesen wird als besonders kritisch eingeschätzt, da hier nicht nur Daten, sondern direkt das Leben von Menschen betroffen ist. Die Interviewten hoben hervor, dass selbst kleine Sicherheitslücken potenziell lebensbedrohliche Auswirkungen haben können. Diese Kritikalität ist untrennbar mit Datenschutzanforderungen verknüpft, da medizinische Daten besonders sensibel sind und gesetzlichen Mindestschutz genießen. |
| Technische Herausforderungen | Technologische Entwicklungen wie die zunehmende Vernetzung (z. B. durch 5G) und Automatisierung (z. B. ferngesteuerte Operationen) erhöhen das Risiko für Angriffe. Viele Einrichtungen kämpfen mit veralteten Systemen, unzureichendem Patchmanagement und Herstellern, die Sicherheitsaspekte unzureichend berücksichtigen. Häufig steht die Nutzerfreundlichkeit im Widerspruch zu Sicherheitsanforderungen, was zu 'Insecurity by Design' führt. |
| Organisationsstruktur | Universitätskliniken haben eine komplexe Struktur aus Forschung, Lehre und medizinischer Versorgung. Diese Vielfalt führt zu dezentralen Zuständigkeiten, die eine einheitliche Umsetzung von Informationssicherheitsmaßnahmen erschweren. Zudem agieren viele Kliniken wie eigenständige Subunternehmen mit eigenen IT- und Sicherheitsstrukturen, was zu Inkonsistenzen führt. |
| Durchsetzung IS-Maßnahmen | Die Einführung und Umsetzung von Sicherheitsmaßnahmen erfolgen häufig ohne ausreichende Einbindung des betroffenen Personals. Dies kann dazu führen, dass Maßnahmen als hinderlich oder sogar kontraproduktiv wahrgenommen werden. Die fehlende Rückkopplung an das IS-Team führt dazu, dass notwendige Anpassungen zu spät oder gar nicht erfolgen. |
| Ressourcenmangel | Der massive Fachkräftemangel betrifft nicht nur die Pflege, sondern auch die IT-Abteilungen. Dadurch fehlen sowohl die personellen Ressourcen zur Umsetzung als auch das Know-how für strategische Weiterentwicklungen. Die Verantwortung für IS wird häufig auf wenige Schultern verteilt, was zu Überlastung und Verzögerungen führt. |
| Faktor Mensch – Risiko | Phishing-Angriffe stellen laut fünf der sechs Interviewten das größte Risiko dar. Typische Einfallstore sind täuschend echt aussehende E-Mails. Neben Unachtsamkeit spielen auch Überforderung und Unwissenheit eine Rolle. Selbst mehrfach kommunizierte Warnungen werden ignoriert, was das Risiko weiter erhöht. |
| Faktor Mensch – Chance | Trotz der Risiken sehen drei der Interviewten im Personal eine zentrale Sicherheitsressource. Mitarbeitende, die geschult und motiviert sind, können potenzielle Angriffe erkennen und verhindern. Besonders wichtig ist dabei die sogenannte 'menschliche Firewall', also ein sicherheitsbewusstes Verhalten im Alltag. Offene Fehlerkultur und klare Meldewege sind dafür entscheidend. |
| ISA-Zielgruppen | Obwohl sieben Zielgruppen identifiziert wurden, konzentrieren sich ISA-Maßnahmen in der Praxis meist auf zwei bis drei Gruppen wie Pflegepersonal, IT oder Verwaltung. Die Inhalte werden oft nicht zielgruppenspezifisch aufbereitet, was deren Wirksamkeit einschränkt. Eine Differenzierung nach Personalgruppen erfolgt kaum. |
| ISA-Ziele | Zentrale Ziele sind der Aufbau eines Grundverständnisses für Informationssicherheit und eine kontinuierliche Sensibilisierung für sicherheitsrelevante Verhaltensweisen. Es soll ein Bewusstsein dafür geschaffen werden, dass Informationssicherheit nicht nur IT betrifft, sondern den gesamten Klinikbetrieb. Dabei sind anschauliche Beispiele und praxisrelevante Inhalte besonders wirksam. |

| Kategorie | Ergebnisse |
|---|---|
| ISA-Probleme | Die größten Herausforderungen liegen im begrenzten Zeitbudget des Personals, besonders im medizinischen Bereich, in der Verwendung generischer und wenig passgenauer Inhalte sowie in mangelnder Unterstützung durch die Leitungsebene. Hinzu kommt die Gefahr, durch zu viele Warnungen eine Abstumpfung gegenüber Sicherheitsrisiken zu erzeugen. |
| Vermittlungsmethoden | Am wirksamsten gelten Online-Trainings (wegen zeitlicher Flexibilität) und lehrergeführte Schulungen (wegen direkter Rückfragen und Interaktion). Klassische Methoden wie Poster oder Flyer wurden als ineffizient beurteilt, da sie wenig Beachtung finden und kaum Handlung auslösen. Eine Kombination aus digitalen und interaktiven Formaten wird als erfolgversprechend eingeschätzt. |
| ISA-Inhalte | Die behandelten Themen umfassen aktuell Datenschutz, Passwortrichtlinien und korrekte Nutzung von E-Mail. Zukünftig sollen vermehrt auch nicht-technische Aspekte wie die Verarbeitung von Papierakten und physische Zugangskontrollen behandelt werden. Entscheidend ist der Praxisbezug, um Aha-Effekte und Selbstwirksamkeit zu fördern. |
| Qualitätssicherung | Zur Sicherstellung der Qualität greifen Einrichtungen auf externe Dienstleister, Fachzeitschriften oder offizielle Behördenquellen wie das BSI zurück. Es besteht ein klar geäußerter Wunsch nach mehr Kooperation mit anderen Stellen wie Patientensicherheit oder Unternehmenskommunikation sowie nach partizipativen Formaten mit dem Klinikpersonal. |
| Evaluation & Messbarkeit | Eine systematische Evaluation von ISA-Maßnahmen findet bisher nicht statt. Stattdessen werden Rückmeldungen informell gesammelt. Ein Hindernis ist die Angst vor Leistungsbewertung und daraus resultierende Konflikte mit dem Personalrat. Dennoch erkennen mehrere Teilnehmende die Notwendigkeit einer besseren Erfolgskontrolle an, um Maßnahmen gezielt weiterentwickeln zu können. |

## Qualitative Ergebnisse aus Workshops zu Hürden und Anreizen im Kontext der Information Security Awareness

Die Workshopreihe zur Erhebung von Hürden und Anreizen im Umgang mit Informationssicherheitsmaßnahmen wurde mit dreizehn Teilnehmerinnen und Teilnehmern aus einem Universitätsklinikum durchgeführt. Die Teilnehmenden repräsentierten eine vielfältige Gruppe medizinischer und technischer Berufsprofile: darunter Ärztinnen und Ärzte, Assistenzärztinnen und Assistenzärzte, Pflegefachpersonen, Ingenieurinnen und Ingenieure, Optometristinnen, Sicherheitsverantwortliche sowie Mitarbeitende aus Verwaltung und Wissenschaft. Das Alter der Teilnehmenden variierte zwischen 20 und über 60 Jahren; sowohl Personen mit wenigen Berufsjahren als auch solche mit jahrzehntelanger Erfahrung nahmen teil. Insgesamt waren vier Frauen und neun Männer beteiligt, von denen fünf eine leitende Funktion ausübten. Die Workshops wurden in Kleingruppen durchgeführt und behandelten zentrale Aspekte wie die Relevanz und Umsetzung von Richtlinien zur Informationssicherheit, konkrete Barrieren im Alltag sowie Kriterien für gelungene Awareness-Maßnahmen.

### Identifizierte Hürden für ISA

Im Ergebnis zeigten sich 14 übergeordnete Themenkategorien mit insgesamt 27 verschiedenen Erklärungen für menschliches Fehlverhalten im Zusammenhang mit

Informationssicherheitsmaßnahmen (sh. Tabelle 4). Zu den häufigsten Hürden zählten Arbeitslast und Zeitdruck, bauliche Einschränkungen, unklare oder schlecht zugängliche Richtlinien, unzureichender technischer Support und ein Mangel an Schulung und Wissen. Die Ergebnisse verdeutlichen, dass viele Maßnahmen als wenig praktikabel oder sogar hinderlich für die medizinische Versorgung empfunden werden. Gleichzeitig zeigten die Diskussionen, dass Mitarbeitende grundsätzlich bereit sind, sich sicherheitskonform zu verhalten, sofern sie die Maßnahmen verstehen, als sinnvoll erleben und dabei unterstützt werden.

**Tabelle 4**: Zentrale Workshopergebnisse zu den ISA-Hürden im medizinischen Arbeitsalltag

| Kategorie | Erläuterung |
|---|---|
| Arbeitslast & Zeitdruck | Multitasking, hoher Zeitdruck sowie die Notwendigkeit ständiger Erreichbarkeit können dazu führen, dass Informationssicherheitsmaßnahmen vernachlässigt werden. |
| Bauliche & räumliche Gegebenheiten | Ungeeignete physische Arbeitsumgebungen beeinträchtigen die sichere Handhabung sensibler Informationen. |
| Betrug & Fehler | Unabsichtliche Fehler können zu Verstößen gegen Informationssicherheitsrichtlinien führen; betont wird die Bedeutung gut erreichbarer IT-Notfalldienste. |
| Fehlende Unterstützung & Voraussetzungen | Mangel an reibungsloser IT-Unterstützung und fehlende leicht verfügbare Ressourcen erschweren den Umgang mit Sicherheitsmaßnahmen. |
| Harmonisierung Prozesse & IS-Maßnahmen | Mangelnde Abstimmung zwischen Arbeitsprozessen und Sicherheitsmaßnahmen kann zu Komplikationen führen. |
| Ignoranz | Fehlende Einsicht in die Notwendigkeit von Sicherheitsmaßnahmen begünstigt nachlässiges Verhalten. |
| Komplexe Prozesse | Undurchsichtige und komplizierte Prozesse führen zu Fehlern und Unsicherheiten im Umgang mit Sicherheitsanforderungen. |
| Mangelnde Disziplin | Menschliche Verhaltensmuster wirken sich negativ auf die konsequente Umsetzung von Sicherheitsmaßnahmen aus. |
| Mangelndes Bewusstsein | Unzureichende Wahrnehmung und Aufmerksamkeit gegenüber Informationssicherheit beeinträchtigen die Umsetzung. |
| Organisationale Kultur & Klima | Vertrauen in die Integrität anderer sowie der Umgang mit vertraulichen Informationen sind zentrale Herausforderungen. |
| Praktikabilität & Effizienz | Sicherheitsmaßnahmen werden hinsichtlich ihres Zeitaufwands und ihrer Vereinbarkeit mit Patientenwohl und Prozessflexibilität kritisch betrachtet. |
| Technologische Aspekte | Usability, lange Zugriffszeiten und IT-Infrastruktur erschweren die Umsetzung von Sicherheitsmaßnahmen. |
| Unwissenheit & fehlende Fähigkeiten | Fehlende IT- und Sicherheitskompetenzen wirken als Barriere bei der korrekten Handhabung. |
| Zugang & Verfügbarkeit von Richtlinien | Unklare Struktur und schlechte Auffindbarkeit von Richtlinien behindern die Umsetzung von Sicherheitsmaßnahmen. |

Die Literatur zu Hürden von ISA in medizinischen Einrichtungen benennt eine Vielzahl von Faktoren, die menschliches Fehlverhalten begünstigen. Dazu zählen insbesondere mangelnde Sensibilisierung und Schulung, informelle Arbeitspraktiken wie das Teilen

von Passwörtern sowie die generelle Priorisierung medizinischer Aufgaben gegenüber sicherheitsbezogenen Anforderungen. Belastende Arbeitsbedingungen, eine schlechte IT-Infrastruktur sowie das Empfinden, Sicherheitsmaßnahmen würden die Produktivität behindern, wirken zusätzlich hemmend [18], [20].
Auch organisationale Schwächen wie fehlende Unterstützung, unklare Zuständigkeiten und das Gefühl von Kontrolle oder Druck durch Richtlinien beeinträchtigen die Einhaltung sicherer Verhaltensweisen [22]. Mitarbeitende rechtfertigen Verstöße oft durch arbeitsbezogene Zwänge oder soziale Dynamiken im Team. Dabei kommt den Kolleginnen, Kollegen und Führungskräften eine prägende Rolle zu [23]. In kollaborativen Arbeitsumgebungen entstehen zudem Unsicherheiten hinsichtlich der Verantwortlichkeit für Datenschutzverstöße [24]. Gleichzeitig fehlt dem IT-Personal oft das Verständnis für informelle Umgehungslösungen, was die Entwicklung geeigneter Gegenmaßnahmen erschwert [25].
Datenschutzbeauftragte betonen die Bedeutung struktureller Faktoren: Ineffiziente Prozesse, mangelnde Kontrolle und die unzureichende Einbindung der Führungsebene gelten als zentrale Ursachen für sicherheitsrelevante Fehler. Schulungen und Awareness-Maßnahmen werden als zentrale Gegenstrategien hervorgehoben [26]. Zusätzlich stellen die hohe Komplexität der IT-Landschaft, heterogene Systemlandschaften sowie begrenzte personelle und finanzielle Ressourcen eine erhebliche Herausforderung für die Umsetzung von Informationssicherheitsmaßnahmen dar [27].
Aus der Literatur und den Workshops ergibt sich ein klares, konsistentes Bild: Die Ursachen für menschliches Fehlverhalten im Bereich der Informationssicherheit in medizinischen Einrichtungen sind vielfach deckungsgleich, zeichnen aber auch ein ergänzendes Bild. Zentrale Problemfelder wie Arbeitsüberlastung, fehlende Schulung, komplexe Abläufe und mangelnde organisationale Unterstützung tauchen sowohl in wissenschaftlichen Studien als auch in der gelebten Praxis des Klinikalltags deutlich auf. Für die Entwicklung wirksamer Awareness-Maßnahmen ist es daher essenziell, eine breite Bandreite identifizierten Hürden systematisch zu adressieren

### Identifizierte Anreize für ISA-Maßnahmen

Im Workshop wurden Anreize identifiziert, die Awareness-Maßnahmen zur Informationssicherheit besonders wirksam und attraktiv machen. Diese Anreize lassen sich fünf Themenfeldern zuordnen und zeigen, was Mitarbeitende motiviert, sich aktiv mit Informationssicherheit auseinanderzusetzen:

- **Sinnstiftung und persönliche Relevanz**
  Transparente, nachvollziehbare Inhalte, die den Nutzen im Arbeitsalltag verdeutlichen, fördern Motivation und aktives Mitdenken.

- **Wahl der Lernformate**
  Interaktive, praxisnahe Formate mit kurzen, prägnanten Inhalten und individueller Anpassbarkeit erhöhen das Engagement.
- **Praxisbezogene Inhalte**
  Aktualität, Alltagsnähe und klare, verständliche Sprache machen Inhalte greifbar und unmittelbar anwendbar.
- **Unterstützende Lernkultur**
  Persönliche Ansprache, eine fehlerfreundliche Lernumgebung und Feedback-Möglichkeiten schaffen Vertrauen und Lernbereitschaft.
- **Strukturelle Erleichterung**
  Zentraler Zugang, klare Struktur und gut auffindbare Materialien erleichtern die Integration ins tägliche Arbeiten und Senken Einstiegshürden.

## Qualitative Ergebnisse potenzieller KPIs zur Messung der Information Security Awareness – Erkenntnisse aus einer Fokusgruppe in einer Universitätsklinik

Im Rahmen einer Fokusgruppe zur Identifikation geeigneter KPIs für ISA in einer Universitätsklinik kamen zehn Teilnehmende aus der IT-Abteilung, dem Bereich der Informationssicherheitsbeauftragten (ISBs) sowie dem Chief Information Security Office (CISO) zusammen. Ziel des Fokusgruppe war es, eine gemeinsame Grundlage zu schaffen, um bestehende sowie potenziell neue Kennzahlen zur Messung und Steuerung von ISA zu bewerten. Dabei wurden sowohl bereits verfügbare Datenquellen identifiziert als auch die Anforderungen an den gewünschten Detaillierungsgrad (z. B. auf Ebene von Endgeräten, Abteilungen oder Stationen) diskutiert. Der Austausch diente dazu, realisierbare und zugleich aussagekräftige KPIs abzuleiten, die künftig zur kontinuierlichen Verbesserung der Sicherheitslage beitragen können.

**Tabelle 5**: Klinikbezogene KPIs zur Bewertung von Awareness und technischer Informationssicherheit

| KPI | Erklärung | Differenzierungsgrad | KPI-Typ |
|---|---|---|---|
| Passwortkomplexität (Länge) | Stärke der gewählten Passwörter zur Zugriffssicherung | Pro Nutzer oder Nutzerin | Awareness |
| Passwortänderungsintervall | Häufigkeit der Passwortwechsel zur Vermeidung langfristiger Kompromittierung | Pro Nutzer oder Nutzerin | Awareness |
| Anzahl gemeldeter Sicherheitsvorfälle | Anzahl registrierter Sicherheitsvorfälle | Gesamte Klinik oder Organisationseinheiten | Awareness |
| Quote der IT-Sicherheitsschulung an Klinik | Anteil des geschulten Personals | Pro Nutzer oder Nutzerin | Awareness |

| KPI | Erklärung | Differenzierungsgrad | KPI-Typ |
|---|---|---|---|
| Informationssicherheitsvorfälle mit menschlichem Fehlverhalten | Vorfälle, bei denen menschliches Versagen eine Rolle spielte | Pro Nutzer oder Nutzerin | Awareness |
| Kenntnis der Meldekette | Bewusstsein des Personals über den Ablauf zur Vorfallsmeldung | Pro Nutzer oder Nutzerin | Awareness |
| Klickraten auf Phishingkampagnen | Anteil der Klicks auf simulierte Phishing-Mails | Pro Nutzer oder Nutzerin | Awareness |
| Clean Desk | Umsetzung von aufgeräumten Arbeitsplätzen zur Datensicherheit | Pro Nutzer oder Nutzerin | Awareness |
| Quote der durch falsches Passwort gesperrten Accounts | Nutzerkonten, die durch wiederholte Falscheingabe gesperrt wurden | Pro Nutzer oder Nutzerin | Awareness |
| Systeme mit 2-Faktor-Authentifizierung | Anteil der Systeme mit zusätzlicher Authentifizierung | Pro System | Technisch |
| Anzahl Wartungsfenster | Anzahl geplanter Wartungszeiträume für Systeme | Nach Systemkategorie oder Zeitintervall | Technisch |
| Anzahl der aktuell gepatchten Systeme | Aktuell auf dem neuesten Stand befindliche Systeme | Nach Systemgruppe oder Kritikalität | Technisch |
| Anzahl Sicherheitsvorfälle | Absolute Anzahl sicherheitsrelevanter Vorfälle | Gesamte Klinik oder Organisationseinheiten | Technisch/Awareness |

Die vorliegende KPI-Tabelle (sh. Tabelle 5) fasst die Ergebnisse der Fokusgruppe zur Bewertung der Informationssicherheitslage in der Klinik zusammen. Sie enthält sowohl verhaltensorientierte Kennzahlen, die das Sicherheitsbewusstsein der Mitarbeitenden abbilden, als auch technische Indikatoren, die den Zustand und die Absicherung der IT-Infrastruktur messbar machen.

Ein zentraler Teil der KPIs lässt sich dem Bereich Security Awareness zuordnen, was auch gezielt in der Fokusgruppe thematisiert wurde. Dazu zählen Kennzahlen wie die Passwortkomplexität, das Passwortänderungsintervall, die Quote geschulter Mitarbeitender oder die Klickrate auf simulierte Phishing-Mails. Solche Metriken machen menschliches Verhalten und den Kenntnisstand der Mitarbeitenden quantifizierbar. Sie ermöglichen es, die Wirksamkeit von Schulungen, Sensibilisierungskampagnen oder internen Richtlinien gezielt zu evaluieren und auf dieser Basis kontinuierlich weiterzuentwickeln.

Ergänzt wird dieses Set durch technisch orientierte KPIs wie die Anzahl aktuell gepatchter Systeme, die Zahl geplanter Wartungsfenster oder den Anteil an Systemen mit implementierter Zwei-Faktor-Authentifizierung. Diese Kennzahlen geben Aufschluss über den technischen Sicherheitsstatus der IT-Systeme und sind eng mit dem Schwachstellenmanagement, der Umsetzung technischer Baselines und dem Schutz vor externen Angriffen verknüpft.

Die Anzahl der registrierten Sicherheitsvorfälle stellt eine Sonderkategorie dar, da sie sowohl durch technische Schwächen als auch durch menschliches Fehlverhalten ausgelöst sein kann. Für eine differenzierte Bewertung ist es notwendig, diese Kennzahl weiter nach Ursache, Schweregrad und betroffener Organisationseinheit zu unterteilen.

Die hier aufgeführten KPIs stellen keine abschließende oder vollständig systematische Auswahl dar. Vielmehr bilden sie einen praxisorientierten Ausgangspunkt zur Bewertung zentraler Aspekte der Informationssicherheit im Klinikbetrieb. Weitere KPIs können je nach Datenverfügbarkeit, Risikoanalyse oder strategischer Zielsetzung ergänzt werden.
Insgesamt dienen die erhobenen KPIs als objektive Grundlage, um sowohl operative Maßnahmen im klinischen Alltag als auch strategische Entwicklungen im Bereich der Informationssicherheit über längere Zeiträume hinweg zu bewerten. Entscheidend ist, dass die Kennzahlen regelmäßig erhoben, in ein geeignetes Beobachtungsdesign eingebettet, im klinischen Kontext interpretiert und gezielt zur Steuerung und Weiterentwicklung von Informationssicherheitsmaßnahmen eingesetzt werden.

## Partizipative Entwicklung von Nudges zur Förderung der Information Security Awareness – Erkenntnisse aus vier Fokusgruppen in einer Universitätsklinik

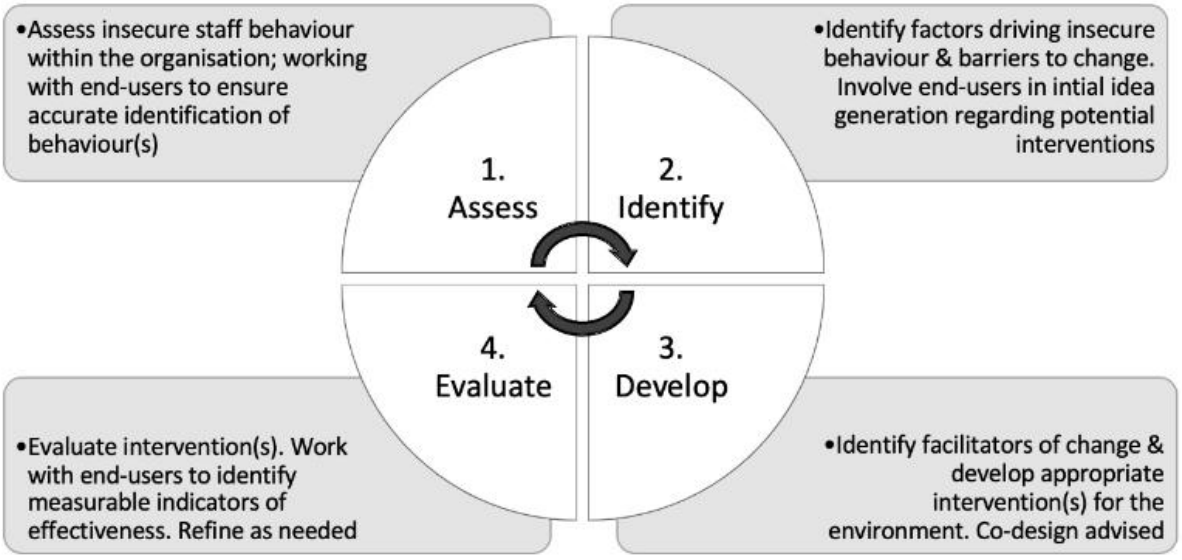
Für die Entwicklung von Nudges haben wir uns am Rahmenwerk des AIDE-Ansatzes (Assess → Identify → Develop → Evaluate) nach Branley-Bell et al. aus dem EU-Horizon Projekt PANACEA orientiert [18] (sh. Abbildung 1) und in einer Universitätsklinik mit insgesamt vier Fokusgruppen angewendet. Der AIDE-Ansatz ist ein strukturierter und zyklischer Prozess zur Entwicklung, Umsetzung und kontinuierlichen Verbesserung von Nudges zur Informationssicherheit, insbesondere im medizinischen Umfeld. Der entscheidende Unterschied zu Vorgängermodellen wie SCENE [28] liegt in der dauerhaften Evaluation und Anpassbarkeit der Maßnahmen. AIDE stellt somit ein vollständiges Framework für evidenzbasierte, praxisnahe Nudging-Projekte dar, das bereits erfolgreich in der Praxis – etwa in medizinischen Einrichtungen – angewendet wurde [18], [29].

AIDE-Schritte im Überblick:

- **Assess**: Analyse der bestehenden organisatorischen Rahmenbedingungen und Verhaltensweisen im sicherheitsrelevanten Kontext.
- **Identify:** Systematische Erfassung unsicherer Verhaltensmuster und deren Ursachen.
- **Develop**: Gestaltung passender Nudges – unter Verwendung des MINDSPACE-Rahmens als heuristische Checkliste für verhaltenspsychologisch wirksame Gestaltungsprinzipien.

- **Evaluate**: Kontinuierliche Evaluation und Optimierung der Maßnahmen anhand klar definierter Metriken. Erfolgreiche Maßnahmen werden verstetigt, nicht wirksame iterativ überarbeitet.

**Abbildung 1**: Der AIDE-Ansatz nach Branley-Bell et al., Seite 7 [15]




Das MINDSPACE-Modell [30], [31] wird im AIDE-Prozess im Develop-Schritt als strukturierende Gestaltungsgrundlage verwendet. Es dient hier als Checkliste zur Ideengenerierung und zur Auswahl geeigneter Interventionen, die psychologisch wirksame Hebel nutzen. Die neun MINDSPACE-Faktoren helfen, Maßnahmen so zu gestalten, dass sie das automatische System menschlichen Entscheidens (nach Kahneman: System 1) effektiv ansprechen [30], [31].
Das MINDSPACE-Rahmenwerk wurde vom Institute for Government (UK) entwickelt und basiert auf Erkenntnissen der Verhaltensökonomie, Psychologie und Nudging-Theorie. Es umfasst folgende neun Einflussfaktoren [30], [31] :

**Tabelle 6**: Das MINDSPACE-Rahmenwerk

| Faktor | Erläuterung |
|---|---|
| Messenger (Sender) | Das Verhalten wird dadurch beeinflusst, von wem eine Information kommuniziert wird. |
| Incentives (Anreize) | Reaktionen auf Anreize werden von vorhersehbaren mentalen Abkürzungen geprägt, wie zum Beispiel starken Verlusten konsequent auszuweichen. Anreize können sowohl Belohnung als auch Bestrafung sein. |

| Faktor | Erläuterung |
|---|---|
| Norms (Normen) | Das Verhalten hängt stark von dem (erwarteten) Verhalten anderer Personen ab. |
| Defaults (Standardoptionen) | Oft wird man sich „dem Strom anschließen" oder voreingestellte oder angebotene Optionen wählen, d.h. man wird sich oft für die Standardoption entscheiden, wenn eine bereitgestellt wird. |
| Salience (Auffälligkeit) | Das Verhalten wird dadurch beeinflusst, dass man sich von Neuem und scheinbar Relevantem in den Bann ziehen lässt |
| Priming (Bahnung) | Handlungen können von unbewussten Hinweisen beeinflusst werden. |
| Affect (Affekt) | Entscheidungen werden von Emotionen geformt, daher kann die emotionale Reaktion auf etwas auch die Handlungen beeinflussen. |
| Commitments (Einsatz, Verbindlichkeit) | Personen streben danach, ihren öffentlichen Versprechen treu zu bleiben und erwidern Handlungen in gleicher Weise. |
| Ego | Das Ego führt dazu, dass Menschen sich auf Arten verhalten, die ihr Selbstbild positiver gestalten lässt. |

**Schritt 1: Assess**

Um die Relevanz kritischer Bereiche der Informationssicherheit (ISA) effizient und gleichzeitig fundiert zu bewerten, wurde der erste Schritt des AIDE-Prozesses angepasst, indem ein qualitativer durch einen quantitativen Ansatz ersetzt wurde. Hierzu kam ein ISA-Fragebogen zum Einsatz, der verschiedene Aspekte der Informationssicherheit abdeckte und ein breites Meinungsbild ermöglichen sollte. Insgesamt nahmen 717 Personen teil, darunter 44 aus dem ärztlichen Dienst und 81 aus dem Pflegedienst (Der verwendete Fragebogen stellte eine vorläufige Version des in Abschnitt 0 beschriebenen psychometrischen Messinstruments dar). Die Auswertung der quantitativen Ergebnisse ergab 9 ISA-Schwerpunkte, die sowohl für die Klinik insgesamt als auch insbesondere für den ärztlichen und pflegerischen Dienst durch die Stabstelle für Informationssicherheit als besonders relevant im Hinblick auf die Kritikalität der Universitätsklinik eingestuft wurden:

- Verwendung eigene Endgeräte oder E-Mailadressen für die Erledigung dienstlicher Aufgaben (BYOD: Bring-Your-Own-Device)
- Auf dem Laufenden bleiben über die Informationssicherheitsrichtlinie
- Meldung sicherheitsrelevanter Vorfälle durch Kolleginnen und Kollegen
- Meldung verdächtiger Vorfälle
- Clean-Desk-Policy
- Freiwilligkeit bei der Meldung von Vorfällen
- Informationssicherheitsrichtlinien werden als Arbeitshindernis wahrgenommen
- Nachlässigkeitskultur im Umgang mit Informationssicherheitsrichtlinien
- Entwicklung von widersprüchlichen Schattenprozessen zu Informationssicherheitsrichtlinien

**Schritt 2: Identify**

In zwei Fokusgruppen mit Angehörigen des ärztlichen Dienstes (n = 3) sowie des Pflegedienstes (n = 5) wurde innerhalb eines Zeitrahmens von zwei bis drei Stunden gemeinsam der Frage nachgegangen, welche alltäglichen Arbeitsabläufe und formalen Arbeitsanweisungen einen negativen Einfluss auf die ISA-Schwerpunkte haben. Grundlage der Diskussion bildete ein strukturierter Leitfaden, der die in Schritt 1 identifizierten ISA-Schwerpunkte systematisch mit den Teilnehmenden aufgriff. Die Themen wurden den Beteiligten zu Beginn der Sitzungen vorgestellt und dienten als Ausgangspunkt, um gemeinsam relevante Arbeitsabläufe zu identifizieren und mögliche Hindernisse im Zusammenhang mit den ISA-Schwerpunkten herauszuarbeiten.

Im Verlauf der Diskussionen zeigte sich, dass überwiegend die Usability der technische IT-Infrastruktur sowie räumliche Gegebenheiten wesentliche Hürden für bestehende Schwachstellen in der Informationssicherheit darstellen. Diese Faktoren lassen sich durch Nudging nicht beheben. Gleichzeitig wurden auf Basis einer qualitativen Inhaltsanalyse jedoch auch Bereiche identifiziert, die sich grundsätzlich für verhaltensbasierte Nudging-Interventionen eignen:

- **Gemeinsame Nutzung von Accounts**:

  Innerhalb eines einzelnen Windows-Accounts werden mehrere Accounts des Krankenhausinformationssystems gleichzeitig verwendet. Dieses Vorgehen widerspricht grundlegenden Sicherheitsanforderungen, da dadurch die Authentizität und Integrität der verarbeiteten Patienten- und Patientinnendaten gefährdet wird. Das notwendige Ein- und Ausloggen wird vom Personal als ineffizient empfunden.

- **Unbeaufsichtigte mobile Arbeitsplätze:**
Mobile Arbeitsplätze bleiben zeitweise unbeaufsichtigt mit offenem Bildschirm auf dem Flur stehen, was ein Sicherheitsrisiko darstellt.

- **Meldeverhalten bei Vorfällen:**
Es besteht eine Kultur der Nachlässigkeit bei der freiwilligen Meldung von Vorfällen, insbesondere bei kleineren Datenschutzverstößen. Problemwahrnehmung fehlt häufig, oder es besteht die Sorge, als Denunziant bzw. Denunziantin zu gelten.

- **Umgang mit verdächtigen Personen:**
Die Entscheidung, verdächtige Personen zu melden, wird individuell getroffen. Aufgrund hoher Arbeitsbelastung werden fremde Personen im Klinikbereich oft nicht wahrgenommen.

- **Geringe persönliche Relevanz von Informationssicherheit:**
Der persönliche Nutzen von Informationssicherheit wird nicht erkannt. Gleichzeitig fehlen spürbare persönliche Konsequenzen bei Nichteinhaltung von Vorgaben.

- **Nichteinhaltung der Clean-Desk-Policy:**
Die Clean-Desk-Policy wird in nicht abschließbaren Räumen, Funktionsräumen oder an unsicheren Ablageorten häufig nicht eingehalten.

- **Ablehnung formaler Schulungsformate:**
Online-Schulungen zur Informationssicherheit werden primär als formale Pflicht und lästige Checklistenanforderung empfunden, nicht als praxisrelevante Lernchance.

**Schritt 3: Develop**

In zwei weiteren Fokusgruppen mit Angehörigen des ärztlichen Dienstes (n = 4) und des Pflegedienstes (n = 3) wurden gezielt mögliche Interventionen und erste Nudge-Ideen zur Förderung der Informationssicherheit entwickelt. Grundlage war ein strukturierter Leitfaden, der sich am MINDSPACE-Modell sowie an den Workshop-Materialien von Branley-Bell orientierte [15].

Im Zentrum stand die Frage, wie sich Nudging-Maßnahmen alltagstauglich in bestehende Arbeitsabläufe integrieren lassen, um die Einhaltung informationssicherheitsrelevanter Richtlinien zu unterstützen, ohne zusätzliche Belastungen für das Personal zu erzeugen. Hierzu wurden die zuvor definierten ISA-Schwerpunkte vorgestellt und in

einer moderierten Brainstorming-Schleife systematisch entlang der MINDSPACE-Dimensionen diskutiert.
Nicht alle Schwerpunkte konnten dabei gleichermaßen konkret mit Interventionen unterlegt werden. In mehreren Fällen blieb die Auseinandersetzung auf einer abstrakteren Ebene, insbesondere wenn Maßnahmen als unrealistisch, strukturell nicht umsetzbar oder wenig anschlussfähig bewertet wurden, beispielsweise bei Clean-Desk-Vorgaben oder technisch aufwendigen Systemlösungen. Trotz offener Diskussionskultur und des Verzichts auf Denkverbote erschwerte dies die Entwicklung konkreter, verhaltensnaher Maßnahmen.
Insgesamt wurden 56 Nudges generiert (sh. Tabelle 7 bis Tabelle 14). Diese basieren sowohl auf den Ergebnissen aus den Workshops als auch auf der konzeptionellen Weiterentwicklung durch das MedISA-Forschungsteam.

**Tabelle 7:** Messenger Nudges

| **Kategorie** | **Beschreibung** |
|---|---|
| **Kritische Arbeitsabläufe** | Führungskräfte übernehmen keine aktive Rolle bei der Vermittlung von Informationssicherheit. Mitarbeitende nehmen eine geringe Verbindlichkeit wahr, da das Thema nicht konsequent von autoritativen Personen kommuniziert oder vorgelebt wird. |
| **Mögliche Interventionen** | Führungskräfte als sichtbare Vorbilder einbinden; regelmäßige Kommunikation über das Thema in Teambesprechungen; Schulungen durch glaubwürdige Multiplikatoren aus dem Arbeitsalltag. |
| **Mögliche Nudges** | |
| M1: ISA-Teambesprechung | Die Stationsleitung eröffnet jede Teambesprechung mit einem kurzen ISA-Beispiel aus dem Alltag und bedankt sich für das sichere Verhalten. |
| M2: ISA-Faktencheck | Einmal pro Woche versendet eine Oberärztin oder ein Oberarzt eine kurze E-Mail mit dem Titel „ISA-Faktencheck“. Diese enthält einen konkreten Praxisfall (z.B. ein vergessenes Logout oder eine Datenschutzpanne). |
| M3: QM-Sicherheitstipp | Die QM-Beauftragte oder der QM-Beauftragte verschickt regelmäßig E-Mails mit kurzen Sicherheitstipps verbunden mit der Botschaft „Ein Klick schützt Patienten und Patientinnen“. |
| M4: ISA-Frühbesprechung | In der Frühbesprechung wird einmal pro Woche ein kurzer Informationsblock zur Datensicherheit von der Gruppenleitung eingebaut verbunden mit Lob oder Rückmeldung. |
| M5: ISA-Zahlen in der Versammlung | Auf der Mitarbeitenden-Versammlung präsentiert der Vorstand oder die Geschäftsleitung reale Zahlen zu offenen Accounts und nennt konkrete Risiken für Patientinnen und Patienten. |
| M6: ISA-Aushang Dienstplan | Am gedruckten Dienstplan hängt ein farbiger Aushang mit einer persönlichen Aussage der Stationsleitung zur Bedeutung von Informationssicherheit. |

| Kategorie | Beschreibung |
|---|---|
| M7: Dankesbrief Klinikleitung | Ein handschriftlich unterzeichneter Brief der Klinikleitung wird an alle Stationen verteilt mit der Botschaft „Wir sehen Ihren Beitrag zur Sicherheit und danken Ihnen persönlich“. |

**Tabelle 8:** Anreiz Nudges

| Kategorie | Beschreibung |
|---|---|
| **Kritische Arbeitsabläufe** | Mitarbeitende erkennen keinen persönlichen oder kollektiven Nutzen bei sicherem Verhalten. Es fehlen erkennbare Vorteile oder Belohnungen, wodurch die Motivation sinkt. |
| **Mögliche Interventionen** | Teamwettbewerbe mit kleinen Belohnungen; positive Verstärker für korrektes Verhalten (z.B. kleine Geschenke oder öffentliches Lob); Gamification von Sicherheitszielen. |
| **Mögliche Nudges** | |
| I1: ISA-Challenge | Team mit den meisten Logouts gewinnt monatlich eine Kleinigkeit. |
| I2: Weihnachtsessen für sichere Station | Die Station mit den besten Ergebnissen erhält ein gemeinsames Weihnachtsessen oder einen Zuschuss für einen Teamausflug. |
| I3: Dankeschön-Box bei null Verstößen | Kleine Dankeschön-Boxen mit Snacks und Getränken werden an Teams verteilt, die im letzten Monat keine Verstöße bei der Informationssicherheit hatten. |
| I4: Klinikzeitung mit Teamfoto | In der Klinikzeitung erscheint ein Artikel über Stationen mit vorbildlichem Sicherheitsverhalten inklusive Teamfoto. |
| I5: Datenschutz-Champion-Plakette | Aufkleber oder kleine Plaketten mit der Aufschrift „Datenschutz-Champion“ werden an Computern oder Teamwägen angebracht. |
| I6: ISA-Bonuspunkte für Meldungen | Personen erhalten ISA-Bonuspunkte für jede korrekt gemeldete Situation, einlösbar gegen kleine Prämien. |
| I7: Ranking im Newsletter | Im Newsletter wird ein Ranking veröffentlicht, das zeigt, welche Station wie viele sichere Arbeitstage in Folge geschafft hat. |

**Tabelle 9:** Normen Nudges

| Kategorie | Beschreibung |
|---|---|
| **Kritische Arbeitsabläufe** | Im Arbeitsalltag werden Informationssicherheitsregeln oft vernachlässigt, da Normen und Standards unklar oder nicht verinnerlicht sind. Neue Mitarbeitende übernehmen bestehende problematische Routinen. |
| **Mögliche Interventionen** | Identifikation und Förderung von Vorbildern im Team; Integration von ISA-Themen in Einarbeitungen; Thematisierung in Stationsübergaben; regelmäßige Feedbackrunden zu sicherem Verhalten. |
| **Mögliche Nudges** | |

| Kategorie | Beschreibung |
|---|---|
| N1: Teamsäulen-Zitat | Auf dem Stationsboard hängen Fotos von Teamsäulen mit einem persönlichen Zitat zu ihrem Umgang mit Informationssicherheit. |
| N2: Willkommenspaket | Neue Beschäftigte erhalten ein Willkommenspaket mit klaren Verhaltensregeln und Aussagen wie „So machen wir das auf dieser Station“. |
| N3: Mentoring-System | Ein Mentoring-System verbindet neue Beschäftigte mit besonders sicher arbeitenden Kolleginnen und Kollegen für die ersten Wochen. |
| N4: Lob in Besprechung | In wöchentlichen Besprechungen wird positiv hervorgehoben, wer in der letzten Woche konsequent sicher gearbeitet hat. |
| N5: Anstecker für Vorbilder | Teamsäulen erhalten kleine Anstecker oder Sticker auf dem Namensschild die ihre Vorbildrolle sichtbar machen. |
| N6: Reflexion von Verstößen | In der Teambesprechung werden reale Verstöße besprochen verbunden mit der Frage „Wie können wir das künftig gemeinsam verhindern“. |
| N7: Best-Practice-Plakate | Eine Plakatreihe stellt Best-Practice-Fälle aus der eigenen Klinik vor mit kurzen Interviews. |

**Tabelle 10:** Default Nudges

| Kategorie | Beschreibung |
|---|---|
| **Kritische Arbeitsabläufe** | Technische Systeme erlauben Verhaltensweisen, die unsicher sind (z. B. kein automatisches Logout, keine Sperrbildschirme). Mitarbeitende werden dadurch nicht zu sicherem Verhalten geleitet. |
| **Mögliche Interventionen** | Technische Voreinstellungen wie automatischer Logout nach 3 Minuten; verpflichtender Sperrbildschirm; reduzierte Notwendigkeit von aktivem Sicherheitsverhalten. |
| **Mögliche Nudges** | |
| D1: Automatisches Logout bei Inaktivität | Alle Arbeitsplätze sind so konfiguriert, dass sie sich automatisch nach drei Minuten Inaktivität abmelden. |
| D2: Voreingestellte sichere Kommunikationssoftware | Kommunikationssoftware mit sicherem Übertragungsstandard ist vorinstalliert und voreingestellt. |
| D3: Kontaktlose Anmeldung mit Auto-Abmeldung | Die Anmeldung erfolgt kontaktlos über eine persönliche Zugangskarte, die auch automatisch abmeldet, wenn sie entfernt wird. |
| D4: Gerätesperre bei Standortwechsel | Mobile Geräte sperren sich automatisch beim Verlassen des Stationsbereichs. |
| D5: Einheitliche Logout-Symbole | Logout-Symbole sind einheitlich gestaltet und an der gleichen Position auf jedem Gerät, um automatisches Verhalten zu erleichtern. |
| D6: Touch-Logout mit LED-Farbe | Touch-Logout-Schaltfläche an mobilen Geräten mit LED-Farbcode. |
| D7: Doppelseitiger Druck voreingestellt | Druckaufträge sind auf doppelseitigen Druck voreingestellt, um Datenschutzrisiken zu verringern. |

**Tabelle 11:** Salience & Priming Nudges

| Kategorie | Beschreibung |
|---|---|
| **Kritische Arbeitsabläufe** | Im stressigen Klinikalltag sind Sicherheitsrisiken oft nicht präsent, da Hinweise zur Informationssicherheit entweder unauffällig platziert oder nicht situationsgerecht gestaltet sind. Dennoch bietet die Arbeitsumgebung zahlreiche Möglichkeiten, durch gezielte Reize das Verhalten unterbewusst in eine sichere Richtung zu lenken. |
| **Mögliche Interventionen** | Durch gezielte Gestaltung der Umgebung mit auffälligen temporären Hinweisen an stark frequentierten Stellen, etwa in Form rotierender Mini-Poster, Tischaufsteller oder farblicher Symbole, kann Informationssicherheit wirksam ins Bewusstsein gerückt werden. Besonders wirkungsvoll sind visuelle Reize, die direkt an relevanten Handlungspunkten platziert sind und durch Wiederholung, Routinen oder sensorische Signale unterbewusst sicheres Verhalten fördern. |
| **Mögliche Nudges** | |
| S&P1: Aufkleber „Bist du ausgeloggt?“ am Bildschirm | Rote Aufkleber mit der Aufschrift „Bist du ausgeloggt?“ werden direkt am Bildschirmrand platziert und erinnern visuell beim Verlassen des Arbeitsplatzes. |
| S&P2: One Minute Wonder am Spiegel | Wöchentlich wechselnde „One Minute Wonder“-Poster mit echtem Risiko oder Fehlerbeispielen werden an Spiegeln in den Personaltoiletten platziert und fördern bewusstes Verhalten. |
| S&P3: Sticker an Kaffeemaschinen | In Pausenräumen kleben an den Kaffeemaschinen humorvoll gestaltete Sticker mit der Botschaft „Kein Kaffee ohne Logout“, die das Thema niedrigschwellig präsent machen. |
| S&P4: Pop-up mit Sicherheitstipp | Beim Einloggen erscheint ein kurzes Pop-up mit Sicherheitstipps wie „Ein Klick schützt mehr als du denkst“. |
| S&P5: QR-Code auf Dienstausweis | Auf dem Dienstausweis ist ein QR-Code angebracht, der zu einer 30-sekündigen Mini-Schulung mit Datenschutz-Basics führt. |
| S&P6: Visueller Logout-Timer am Desktop | Ein visueller Timer auf dem Desktop zeigt an, wie lange ein Arbeitsplatz ohne Logout aktiv war. |
| S&P7: QR-Code-Sticker zu Sicherheitsregeln | QR-Code-Sticker für schnelle Tipps zu Sicherheitsregeln werden an relevanten Orten der Informationssicherheit angebracht. |

**Tabelle 12:** Affekt Nudges

| Kategorie | Beschreibung |
|---|---|
| **Kritische Arbeitsabläufe** | Mangelndes Verantwortungsgefühl und fehlende emotionale Verbindung zu Informationssicherheitsverstößen. |
| **Mögliche Interventionen** | Fallbeispiele emotional aufbereiten (z B. unbefugter Zugriff auf Patienten- und Patientinnendaten); Reflexion der persönlichen Verantwortung bei Besprechungen; Visualisierung möglicher Folgen. |

| Kategorie | Beschreibung |
|---|---|
| **Mögliche Nudges** | |
| A1: Poster mit realem Vorfall | Ein Poster schildert den anonymisierten Fall eines Mitarbeitenden, der durch einen vergessenen Logout bloßgestellt wurde. |
| A2: Video mit Patientin zur Datensicherheit | In einem Video berichtet eine Patientin, wie sie sich fühlte, als ihre Daten ungeschützt einsehbar waren. |
| A3: Aufkleber mit Datenschutzfrage | Aufkleber an Arbeitsplätzen fragen: „Würdest du wollen, dass jemand deine Daten sieht?“. |
| A4: Reflexionskarten in der Pause | In der Pause liegen Reflexionskarten zur Informationssicherheit aus mit der Frage: „Was, wenn das deine Familie betrifft?“ aus. |
| A5: Spiegel-Aufkleber zur Eigenbetroffenheit | In Pausenräumen oder im Personal-WC hängen kleine Spiegel mit einem dezenten Aufkleber, der die Frage stellt: „Wenn es deine Gesundheitsdaten wären, würdest du wollen, dass jemand darüber spricht?“ |
| A6: Comic-Plakate mit Konsequenz | Comicartige Plakate zeigen Alltagsfehler mit Konsequenzen wie „Der vergessene Logout“. |
| A7: Soundeffekt bei Logout | Beim erfolgreichen Logout wird ein freundlicher Soundeffekt abgespielt, der die Aktion positiv verstärkt. |

**Tabelle 13**: Commitment Nudges

| Kategorie | Beschreibung |
|---|---|
| **Kritische Arbeitsabläufe** | Unterschriften oder Schulungsteilnahmen werden als reine Formalität wahrgenommen, ohne echte Verbindlichkeit oder Reflexion. |
| **Mögliche Interventionen** | Verpflichtende Teamziele; persönliche Versprechen oder Absprachen im Team; Integration in Zielvereinbarungen mit Führungskräften. |
| **Mögliche Nudges** | |
| C1: Unterschrift bei Einarbeitung | Bei der Einarbeitung unterschreiben neue Mitarbeitende eine Verpflichtung zur Informationssicherheit, die regelmäßig erneut vorgelegt wird. |
| C2: Rotes Sticker-Board im Stationszimmer | Auf einem Board im Stationszimmer wird täglich anonym mit einem roten Sticker dokumentiert, wie häufig sich jemand nicht korrekt abgemeldet hat. |
| C3: Sicherheitskarte mit Checkboxen | Mitarbeitende erhalten eine kleine, laminierte Karte für die Kitteltasche mit der Aufschrift „Mein Sicherheitsritual im Alltag“, auf deren Rückseite sie verschiedene Verhaltensziele per Checkbox abhaken können. |
| C4: Team-Codewort zur Erinnerung | Das Team einigt sich auf ein gemeinsames, unauffälliges Codewort oder eine Geste, um Kolleginnen und Kollegen im Alltag freundlich an informationssicheres Verhalten zu erinnern, zum Beispiel „Fenster offen?“ als Hinweis auf ein vergessenes Logout. |
| C5: Team-Miniverträge sichtbar aufhängen | Stationen entwickeln eigene Miniverträge zur Informationssicherheit die im Team sichtbar aufgehängt werden. |
| C6: Logout-Feld auf Übergabeprotokollen | Auf den Übergabeprotokollen ist ein Feld enthalten das den letzten Logout dokumentiert. |
| C7: Online-Quiz mit Urkunde | Alle Mitarbeitenden absolvieren ein Online-Quiz und erhalten eine Urkunde als sichtbares Zeichen ihrer Verpflichtung zur Informationssicherheit. |

**Tabelle 14:** Ego Nudges

| Kategorie | Beschreibung |
|---|---|
| **Kritische Arbeitsabläufe** | Sicheres Verhalten wird nicht mit einem positiven Selbstbild verknüpft. Es fehlt an Anerkennung für verantwortungsvolles Handeln im Team. |
| **Mögliche Interventionen** | Positive Verstärkung verantwortungsvoller Verhaltensweisen; Rollenmodelle hervorheben; Wettbewerbe wie 'ISA-Held der Woche'; Team-Challenges mit Sichtbarkeit im Intranet. |
| **Mögliche Nudges** | |
| E1: Held/Heldin des Monats | Einmal im Monat wird eine Person im Team genannt, die durch besonders umsichtiges Verhalten (z.B. Meldung eines Risikos) aufgefallen ist. |
| E2: ISA-Siegel bei Teilnahme | Mitarbeitende dürfen auf Wunsch ein ISA-Siegel oder Symbol auf Teamlisten, Schichtplänen oder E-Mail-Signaturen nutzen, wenn sie an einer freiwilligen Schulung zur Informationssicherheit teilgenommen haben. |
| E3: Hinweis auf Befundunterlagen | Auf Monitoren, Befundausdrucken oder in Befundmappen befindet sich ein unauffälliger, aber gut platzierter Hinweis: „Bei Patientinnen und Patienten erkennst du Auffälligkeiten sofort. Informationssicherheit beginnt mit derselben Aufmerksamkeit." |
| E4: Smiley-Terminal zur Selbsteinschätzung | Mitarbeitende bewerten ihr Sicherheitsverhalten am Ende der Schicht über ein Smiley-Terminal mit der Frage: „Wie sicher hast du heute mit sensiblen Daten gearbeitet?" Bei positiven Rückmeldungen erscheint ein kurzer Hinweis wie „Danke, dass Sie Verantwortung übernehmen." |
| E5: Aufsteller am Arbeitsplatz mit Botschaft | Ein kleiner Aufsteller am Arbeitsplatz mit dem Satz: "Sicherheit beginnt nicht bei der IT, sondern beim eigenen Verhalten." |
| E6: Spiegel mit Ruf-Botschaft | In der Umkleide hängt ein Spiegel mit der Aufschrift: „Du schützt nicht nur sensible Daten, du schützt auch deinen Ruf." |
| E7: Aufkleber auf Dienstausweis | Ein dezenter Aufkleber auf dem Dienstausweis: „Informationssicherheit ist mein Standard." |

Bevor einzelne Interventionen in die Umsetzung überführt werden, ist als Ausblick die Anwendung eines standardisierten Kriterienrasters vorgesehen. Dieses soll dabei unterstützen, die identifizierten Nudges hinsichtlich ihrer Umsetzbarkeit, Wirksamkeit und Anschlussfähigkeit in Bezug auf eine konkrete Einrichtung zu bewerten und gemeinsam mit den Anwendern und Anwenderinnen priorisierte Prototypen für die Weiterentwicklung bzw. Einführung auszuwählen [15].

### Schritt 4: Evaluate

Die Evaluation der Wirksamkeit der entwickelten Nudges konnte im Rahmen des Projekts nicht mehr durchgeführt werden, da Schritt 3 erst kurz vor Projektende umgesetzt werden konnte. Zukünftige Forschung kann hier ansetzen, indem geeignete Nudges in Untersuchungsdesigns eingebettet werden, um deren Effektivität sowie deren zeitliche Wirksamkeit systematisch zu überprüfen und wissenschaftlich zu belegen.

## Studie zu Effekten von Nudging auf Sicherheitsmüdigkeit

Die Studie untersuchte, ob Nudging geeignet ist, Sicherheitsmüdigkeit zu verringern. Diese tritt auf, wenn Menschen durch wiederholte oder komplexe Sicherheitsanforderungen mental erschöpft sind. Das kann dazu führen, dass sie Sicherheitsregeln ignorieren oder umgehen. Besonders im Bereich der Passwortsicherheit ist dieses Phänomen gut dokumentiert. Vorgaben wie häufige Passwortänderungen oder komplexe Zeichenanforderungen können zu kognitiver Überforderung führen und letztlich unsicheres Verhalten begünstigen, etwa durch die Wiederverwendung schwacher oder leicht merkbarer Passwörter (vgl. [32], [33], [34], [35]).
Obwohl es bereits viele Studien zur Wirkung von Nudging auf sicherheitsbezogenes Verhalten und zur Sicherheitsmüdigkeit gibt, wurde bislang kaum untersucht, wie beide Konzepte miteinander zusammenhängen. Diese Forschungslücke ist relevant, da Nudging als einfache und kostengünstige Maßnahme gelten kann, um Sicherheitsmüdigkeit zu begegnen, ohne bestehende Sicherheitssysteme grundlegend verändern zu müssen.
Für die Studie wurde ein Online-Experiment mit 487 Teilnehmenden aus den USA durchgeführt. Dabei wurden verschiedene Bedingungen getestet, die Kombinationen aus künstlich erzeugter Sicherheitsmüdigkeit (durch CAPTCHAs) und Nudging-Ansätzen beinhalteten. Erhoben wurden unter anderem emotionale Zustände, wahrgenommene kognitive Belastung sowie die Qualität der erstellten Passwörter.
Die Ergebnisse zeigen, dass anreizbasierte Nudges, die etwa Belohnungssignale oder positive Konsequenzen in Aussicht stellen, sowohl die Passwortqualität verbessern als auch die wahrgenommene Belastung geringhalten können. Motivationsbasierte Nudges, die an persönliche Verantwortung oder soziale Normen appellieren, führten hingegen zu einer erhöhten mentalen Belastung. Dennoch zeigten sich auch bei diesen Nudges positive Effekte auf die Passwortstärke.
Das weist auf ein Spannungsfeld hin. Zwar tragen beide Nudge-Typen zu sichererem Verhalten bei, motivationsbasierte Nudges könnten jedoch langfristig zu stärkerer Erschöpfung führen, was im Rahmen der Ego-Depletion-Theorie als problematisch gilt (vgl. [31]). Teilnehmende berichteten, dass sie sich durch die Nudges dazu gedrängt fühlten, besonders komplexe Passwörter zu wählen, die sie sich kaum merken konnten. Das kann ein Hinweis darauf sein, dass Nudging nicht nur nützlich, sondern auch kognitiv belastend und schwer zu ignorieren ist.
Aus ethischer Sicht unterstreichen die Ergebnisse die Notwendigkeit eines vorsichtigen und reflektierten Einsatzes von Nudges in sicherheitskritischen Kontexten. Besonders bei motivationsbasierten Nudges sollte berücksichtigt werden, dass sie unbeabsichtigt

zur Erschöpfung derjenigen Ressourcen beitragen können, die für sicheres Verhalten eigentlich gefördert werden sollen.

## Ergebnisse zu Phishing Simulation an einer Universitätsklinik: Phishinganfälligkeit der Personalgruppen sowie wirksame ISA-Maßnahmen

Im Rahmen eines groß angelegten Phishing-Simulationsprojekts in einem deutschen Universitätsklinikum wurden zwei aufeinander abgestimmte Studien durchgeführt, um die Ursachen und Gegenmaßnahmen für Phishing-Anfälligkeit unter Krankenhauspersonal systematisch zu erfassen. Ziel war es, sowohl die Wirkung spezifischer E-Mail-Gestaltungsmerkmale auf das Verhalten der Mitarbeitenden zu analysieren als auch die Effektivität gängiger technischer Sicherheitsindikatoren zu evaluieren, die auch als Nudges aufgefasst werden können. Die Besonderheit dieser Untersuchung liegt in ihrer praktischen Relevanz für den Klinikalltag: Beide Studien wurden unter realen Bedingungen und mit einer heterogenen Belegschaft durchgeführt, wobei sowohl menschliche Faktoren als auch technische Rahmenbedingungen berücksichtigt wurden. Während Studie I die psychologischen und kontextuellen Einflussfaktoren auf das Phishing-Anfälligkeiten des Personals untersuchte, konzentrierte sich Studie II auf konkrete, technisch umsetzbare Schutzmaßnahmen. Beide Studien liefern gemeinsam fundierte und differenzierte Erkenntnisse für die Entwicklung praxisnaher Sicherheitsstrategien im Gesundheitswesen.

**Zusammenfassung von Studie I: Einfluss von E-Mail-Gestaltung auf Phishing-Anfälligkeit im Krankenhaus**

Studie I untersuchte, welche Merkmale von Phishing-E-Mails das Verhalten von Krankenhausmitarbeitenden besonders beeinflussen und damit die Wahrscheinlichkeit erhöhen, dass sie auf eine Phishing-Nachricht hereinfallen. Dazu wurde ein experimentelles Design (Plackett-Burman [19]) mit zwölf verschiedenen E-Mail-Varianten eingesetzt, die sich systematisch in zehn Merkmalen unterschieden. Die erste Kampagne umfasste 7.041 Personen, die auf vier Personalgruppen verteilt waren: Ärztlicher Dienst, Pflege- und Funktionsdienst, Verwaltung & IT sowie sonstiges Personal (darunter Medizinisch-Technischer Dienst, Versorgung – z. B. Desinfektion, Küche, Wäsche –, Haustechnik, Versorgungsdienste sowie unterstützende Dienste wie Seelsorge, Personalbetreuung, Kinderbetreuung und weitere Unterstützungs-Rollen). Jede Personalgruppe wurde wiederum in zwölf gleich große Subgruppen aufgeteilt, sodass jede E-Mail-Variante einmal pro Personalgruppe getestet werden konnte (Gruppengröße zwischen 100 und 225 Personen).

Die Ergebnisse zeigten eine insgesamt hohe Anfälligkeit: 31 Prozent der Mitarbeitenden klickten auf den Link in der Phishing-Mail, 26 Prozent gaben auf der gefälschten Anmeldeseite ihre Zugangsdaten ein. Die sogenannte Click-to-Login-Rate lag bei über 85 Prozent, was bedeutet, dass der Großteil derjenigen, die klickten, auch tatsächlich sensible Daten eingab. Die Anfälligkeit variierte zwischen den Personalgruppen, wobei Pflege- und Funktionsdienst am häufigsten betroffen waren. Eine Zeitverlaufsanalyse ergab, dass die meisten Reaktionen innerhalb der ersten 24 Stunden nach Versand der E-Mail erfolgten, jedoch auch eine zweite Aktivitätswelle am folgenden Werktag beobachtet wurde.

Tabelle 15 der Studie zeigt die durchschnittliche Wahrscheinlichkeit (Average Marginal Effects, AMEs) der einzelnen E-Mail-Merkmale, dass Mitarbeitende ihre Login-Daten preisgeben. Dabei wurde deutlich, dass bereits kleine Unterschiede in der E-Mail-Gestaltung große Auswirkungen auf das Login-Verhalten haben können. Der Zeitpunkt des E-Mail-Versands spielte eine wichtige Rolle: E-Mails, die am Morgen verschickt wurden, führten zu signifikant mehr Loginversuchen als solche am Nachmittag. Dieser Effekt war insbesondere beim ärztlichen Dienst und bei der Gruppe Sonstige stark ausgeprägt, mit Reduktionen der Login-Wahrscheinlichkeit um bis zu 13,5 beziehungsweise 10,3 Prozentpunkten bei Nachmittagsversand.

Auch der thematische Kontext der E-Mail hatte einen erheblichen Einfluss. Nachrichten mit Bezug zur Gehaltsabrechnung erhöhten die Login-Rate im Schnitt um 5,5 Prozentpunkte im Vergleich zu technisch neutralen E-Mails, etwa zur Outlook-Kontoaktivierung. Besonders deutlich war dieser Effekt beim ärztlichen Dienst mit einem Anstieg von 9,8 Prozentpunkten sowie bei sonstigem Personal mit 8,1 Prozentpunkten. Auffällig war zudem, dass Plain-Text E-Mails eine höhere Wirkung hatten als solche im HTML-Format. Dies widerspricht der weit verbreiteten Annahme, dass visuell ansprechende E-Mails gefährlicher sind, und deutet darauf hin, dass Mitarbeitende möglicherweise einfache Formatierung mit interner Kommunikation gleichsetzen und deshalb weniger misstrauisch reagieren.

Die emotionale und rhetorische Gestaltung der E-Mails beeinflusste das Verhalten ebenfalls erheblich. Besonders der sogenannte Loss Frame, also die Formulierung von Verlusten bei Nicht-Handeln, steigerte die Login-Rate signifikant. Der Effekt war im Durchschnitt 6,7 Prozentpunkte höher als bei E-Mails, die im Gewinnkontext formuliert waren. Dieser Unterschied war insbesondere bei Pflegepersonal, Verwaltung und sonstigem Personal statistisch signifikant. Auch Dringlichkeitsformulierungen hatten eine Wirkung, insbesondere auf den ärztlichen Dienst, bei dem die durchschnittliche Wahrscheinlichkeit einer Anmeldung um fast acht Prozentpunkte anstieg, wenn eine Dringlichkeit suggeriert wurde.

Weitere Merkmale wie personalisierte Anrede oder der Absender (intern versus extern) hatten nur in bestimmten Gruppen signifikante Effekte. Eine persönliche Ansprache erhöhte etwa bei Pflegepersonal die Login-Rate um 6,2 Prozentpunkte, während sie in anderen Gruppen keine Wirkung zeigte. Ob der Absender intern oder extern war, hatte dagegen durchweg keinen nennenswerten Einfluss.

Insgesamt zeigt Studie I, dass Phishing-Anfälligkeit im Krankenhauskontext stark durch Gestaltung, Kontext und Timing der E-Mail beeinflusst wird. Tabelle 15 macht deutlich, dass kein einzelnes Merkmal allein ausschlaggebend ist, sondern dass Kombinationen kleiner Unterschiede zu erheblichen Verhaltensänderungen führen können. Die Resultate unterstreichen, wie wichtig es ist, Phishing-Risiken differenziert nach inhaltlichen und gestalterischen Faktoren zu analysieren und nicht nur aggregierte Klick- oder Login-Raten zu betrachten. Für die Praxis bedeutet das, dass Schulungen und Schutzmaßnahmen deutlich gezielter an den typischen Mustern von Phishing-Nachrichten sowie an der berufsspezifischen Wahrnehmung von Mitarbeitenden ausgerichtet werden sollten.

**Tabelle 15:** Average Marginal Effects verschiedener E-Mail-Charakteristika für die Preisgabe von Login-Daten

| Kategorie | E-Mail Charakteristika | Gesamt | Ärztlicher Dienst | Pflege & Funktionsdienst | Verwaltung & IT | Sonstiges Personal |
|---|---|---|---|---|---|---|
| Zeitlicher Versand | Freitag vs. Montag | 0,027* | −0,002 | 0,060** | 0,037 | 0,004 |
| | Nachmittag vs. Morgen | −0,056*** | −0,135*** | −0,009 | −0,024 | −0,103*** |
| Kontext & Präsentation | Gehaltsabrechnung vs. E-Mail-Konto | 0,055*** | 0,098*** | 0,037 | 0,023 | 0,081*** |
| | HTML vs. Nur-Text | −0,049*** | −0,092** | −0,034 | −0,036 | −0,064** |
| | Personalisierte vs. generische Anrede | 0,022 | 0,018 | 0,062** | −0,027 | −0,008 |
| | Interner vs. Externer Absender | 0,002 | 0,029 | −0,017 | 0,029 | 0,003 |
| Ton & Ansprache | Gewinn- vs. Verlustdarstellung | −0,067*** | −0,014 | −0,068*** | −0,086** | −0,074** |
| | Dringlichkeit vs. Keine | 0,029* | 0,078* | 0,005 | 0,036 | 0,044 |
| | Glaubwürdige Autorität vs. Keine | 0,029* | 0,048 | 0,000 | 0,011 | 0,074** |
| | Starke Emotionen vs. Keine | −0,016 | −0,038 | 0,028 | −0,063 | −0,035 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Pseudo-$R^2$ Nagelkerke | 0,032 | 0,079 | 0,026 | 0,039 | 0,072 |
| Weitere Statistiken | AUC | 0,594 | 0,649 | 0,583 | 0,609 | 0,645 |
| | n | 7041 | 1199 | 2700 | 1199 | 1943 |

Anmerkung: *p < .05, **p < .01, ***p < .001 (statistische Signifikanz, Holm-korrigiert). Positive Werte bedeuten eine erhöhte Wahrscheinlichkeit, Login-Daten einzugeben; negative Werte eine reduzierte Wahrscheinlichkeit.

**Zusammenfassung von Studie II: Wirkung von Anti-Phishing-Nudges zur Reduktion von Phishing-Anfälligkeit im Krankenhaus**

In Studie II wurde untersucht, wie wirksam konkrete technische Maßnahmen als verhaltenslenkende Hinweise in Form von Anti-Phishing-Nudges eingesetzt werden können, um die Anfälligkeit für Phishing-Angriffe beim Krankenhauspersonal zu reduzieren. Die Studie fand erneut an der gleichen deutschen Universitätsklinikum wie Studie I statt und umfasste 7044 Beschäftigte aus vier Personalgruppen. Innerhalb jeder Gruppe wurden die Personen zufällig auf zwölf Subgruppen verteilt. Eine Subgruppe pro Personalgruppe erhielt eine Phishing-E-Mail ohne jegliche Sicherheitsmaßnahme und diente als Kontrollgruppe. Die anderen elf Gruppen erhielten eine inhaltlich identische E-Mail, allerdings jeweils versehen mit genau einer technischen Intervention. Ziel war es, Maßnahmen zu testen, die sich leicht mit bestehenden IT-Systemen umsetzen lassen und keine tiefgreifenden technischen Eingriffe erfordern.

Alle getesteten Maßnahmen lassen sich als digitale Nudges interpretieren, die nicht durch Zwang oder Blockierung, sondern durch subtile Umgestaltung der Situation Verhalten in Richtung größerer Sicherheit lenken. Die Ergebnisse dieser Interventionen sind in Tabelle 16 zusammengefasst. Besonders effektiv waren visuelle Warnhinweise in Form von Phishing-Bannern. Einfache HTML-Banner reduzierten die Login-Rate im Vergleich zur Kontrollgruppe um 80 Prozent. Plaintext-Banner erzielten eine ähnlich starke Reduktion. Die Kombination eines HTML-Banners mit dem Hinweis auf eine nicht verifizierte Absenderadresse senkte die Login-Rate sogar um 94 Prozent. In einzelnen Personalgruppen wie der Ärztliche Dienst oder der Verwaltung führten diese Maßnahmen dazu, dass keine einzige Anmeldung mehr erfolgte. Diese Banner wirkten wie digitale Hinweiszeichen und riefen zur Achtsamkeit auf, ohne die Handlungsmöglichkeiten einzuschränken.

Auch Maßnahmen, die den Handlungsfluss gezielt unterbrechen, zeigten starke Effekte. Das Platzieren der E-Mails im SPAM-Ordner führte zu einer durchschnittlichen Reduktion der Login-Rate um 90 Prozent. Die Maßnahme funktioniert als Kontext-Nudge: Durch die Verlagerung des Ortes der Nachricht wird ihre Relevanz und Glaubwürdigkeit auf unaufdringliche Weise infrage gestellt. Ebenso effektiv war das Deaktivieren der in der E-Mail enthaltenen Links. Diese Maßnahme reduzierte die Anmeldungen um etwa

61 Prozent. Sie zwang die Empfängerinnen und Empfänger, ihre gewohnte Handlung zu unterbrechen, und ermöglichte so einen Moment der bewussten Reflexion.
Die sogenannte aktive Warnseite, die nach dem Klick auf den Link erschien, wirkte als zusätzlicher Nudge durch visuelles Feedback und verstärkte kognitive Aktivierung. Sie führte zu einer durchschnittlichen Reduktion der Login-Rate um 44 Prozent und war besonders in der Personalgruppe des sonstigen Personals wirksam, bei denen die Login-Rate um 70 Prozent sank. Diese Intervention griff erst nach dem Klick, zeigte aber, dass selbst ein kurzer Moment des Innehaltens noch verhindern kann, dass Zugangsdaten preisgegeben werden.
Andere Maßnahmen, wie die Unterdrückung des Anzeigenamens im Absenderfeld oder das Kennzeichnen mit EXTERN-Tags im E-Mail-Betreff, im Absender oder im Textkörper, zeigten gemischte Resultate. In der Gesamtheit waren ihre Effekte deutlich schwächer oder statistisch nicht signifikant. Besonders die sonstige Personalgruppe profitierte jedoch auch von diesen Nudges, zum Beispiel durch eine Reduktion der Login-Rate um 51 Prozent beim Ausblenden des Absendernamens. Die Kombination aller drei externen Markierungen – im Absenderfeld, Betreff und als Banner – senkte die Login-Rate in der Gruppe der Pflegekräfte um 62 Prozent und in der Gruppe des sonstigen Personals um 67 Prozent. Die Wirkung dieser zusammengesetzten Hinweise war stärker als die einzelnen Elemente, was zeigt, dass Nudges in Kombination gezielter wirken können als isolierte Signale.
Besonders hervorzuheben ist jedoch, dass eine der gängigsten und am weitesten verbreiteten Maßnahmen in der Praxis, nämlich das Kennzeichnen externer E-Mails mit dem Zusatz „[EXTERN]“, in dieser Studie weitgehend wirkungslos blieb. Ob als Betreff-Tag, im Absenderfeld oder im Textkörper – isolierte externe Markierungen führten zu keiner signifikanten Reduktion der Login-Rate. Selbst in Kombination mit anderen Hinweisen, etwa als Teil eines Banners, war der Effekt moderat und abhängig von der Personalgruppe. Dies ist besonders bemerkenswert, da viele Organisationen standardmäßig auf genau diese Maßnahme setzen und sie als vermeintlich effektiven Schutz betrachten. Die Studie zeigt jedoch deutlich, dass dieser Hinweis allein häufig übersehen oder ignoriert wird und in seiner aktuellen Form keine verlässliche Schutzwirkung entfaltet. Er erfüllt damit nicht die Erwartungen an einen funktionierenden Nudge, da er offenbar weder zur bewussten Risikowahrnehmung noch zur Verhaltensänderung führt.
Insgesamt zeigt Tabelle 16, dass Nudges, die visuelle Aufmerksamkeit erzeugen, den Handlungskontext subtil verschieben oder automatisierte Abläufe unterbrechen, stark dazu beitragen können, riskantes Verhalten im Umgang mit Phishing-E-Mails zu verhindern. Besonders hervorzuheben ist, dass alle wirksamen Maßnahmen die Entscheidungsfreiheit des Personals unangetastet ließen. Sie veränderten lediglich die

Rahmung der Situation, in der sicherheitsrelevante Entscheidungen getroffen wurden. Diese Art von interventionsarmem Risikomanagement ist besonders im Krankenhauskontext wertvoll, da Arbeitsabläufe oft stark getaktet und ressourcenbeschränkt sind. Nudges ermöglichen es, Sicherheit zu erhöhen, ohne Prozesse zu verlangsamen oder Vertrauen zu untergraben. Studie II liefert damit einen fundierten empirischen Beleg dafür, dass verhaltensorientierte IT-Sicherheit durch gezielte, situationsbezogene Hinweise wirksam und praxistauglich realisierbar ist.

**Tabelle 16:** Wirksamkeit verschiedener Anti-Phishing-Maßnahmen gemessen als relative Reduktion der Login-Raten

| Kategorie | Bedingung | n | Gesamt | Ärztlicher Dienst | Pflege & Funktions-dienst | Verwaltung & IT | Sonstiges Personal |
|---|---|---|---|---|---|---|---|
| | | | | | Login-Raten | | |
| | Kontrollgruppe | 587 | 0,165 | 0,170 | 0,129 | 0,120 | 0,241 |
| | | | $Relative\ Reduktion = 1 - \frac{Login\text{–}Rate\ Interventionsgruppe}{Login\text{–}Rate\ Kontrollgruppe}$ | | | | |
| Heuristik | Anzeigenamen unterdrücken | 587 | −0,175 | −0,118 | 0,034 | 0,333 | −0,513** |
| [Extern] Kennzeichnung | Absenderfeld (FROM) | 587 | −0,237 | −0,059 | −0,207 | 0,500 | −0,487** |
| | Betreffzeile | 587 | −0,165 | 0,000 | −0,103 | 0,250 | −0,410* |
| | Banner im E-Mail-Text | 587 | −0,526*** | −0,353 | −0,414 | −0,583 | −0,667*** |
| | Kombiniert (Absender, Betreff, Banner) | 587 | −0,577*** | −0,588 | −0,621** | −0,250 | −0,641*** |
| Warnhinweise | HTML-Banner | 587 | −0,804*** | −0,941*** | −0,759*** | −0,750* | −0,795*** |
| | Einfacher Text-Banner | 587 | −0,825*** | −0,765** | −0,759*** | −0,917** | −0,872*** |
| | HTML + Hinweis „Nicht vertrauensw. Absender“ | 587 | −0,938*** | −1,000*** | −0,828*** | −1,000** | −0,974*** |
| Friktions-Maßnahmen | SPAM-Ordner-Zustellung | 587 | −0,897*** | −0,882*** | −0,862*** | −1,000** | −0,897*** |
| | Link deaktiviert | 587 | −0,608*** | −0,765** | −0,621** | −0,083 | −0,692*** |
| | Aktive Warnseite | 587 | −0,443*** | −0,118 | −0,379 | −0,250 | −0,692*** |
| | n | 7044 | | 1200 | 2700 | 1200 | 1944 |

Anmerkung: *p < 0,05, **p < 0,01, ***p < 0,001. Die statistischen Vergleiche basieren auf dem Chi-Quadrat-Test nach Pearson mit Yates-Korrektur für Kontinuität. Dabei wird jede Interventionsgruppe mit der jeweiligen Kontrollgruppe innerhalb derselben Spalte verglichen.

## Validierungsstudie zur psychometrischen und effizienten Messung von ISA mit dem sHAIS-Q

Im Folgenden werden die Ergebnisse der Entwicklung und Validierung eines effizienten psychometrischen Messinstruments für die Erfassung der kognitiven ISA vorgestellt. Zahlreiche etablierte Instrumente zur Erfassung allgemeiner ISA wie der Human Aspects of Information Security Questionnaire (HAIS-Q) [36], der Users' Information Security Awareness Questionnaire (UISAQ) [37], die Security Behavior Intentions Scale (SeBIS) [38] oder die Four Measurement Scales [39] bieten wertvolle Beiträge zur ISA-Forschung. Diese Skalen sind jedoch häufig zu umfangreich, um in zeitkritischen Anwendungsfeldern, wie beispielsweise in medizinischen Versorgungseinrichtungen, praktikabel eingesetzt zu werden. Gerade in solchen Umgebungen besteht ein hoher Bedarf an Instrumenten, die ISA als latente Dimension effizient, valide und theoriegeleitet erfassen können. Eine aktuelle systematische Übersichtsarbeit zeigt zudem, dass die Mehrheit der verfügbaren ISA-Skalen nicht den grundlegenden Kriterien methodischer Strenge entspricht [40]. Vor diesem Hintergrund wurde der Short HAIS-Q (sHAIS-Q) entwickelt: Eine kompakte, theoretisch und psychometrisch fundierte Kurzversion des HAIS-Q, die eine effiziente Erhebung von ISA erlaubt.

**Das Knowledge–Attitude–Behavior Modell als theoretische Fundierung**

Das KAB-Modell (Knowledge–Attitude–Behavior) ist ein geeignetes Rahmenmodell mittlerer Reichweite für die Operationalisierung von ISA. Es geht davon aus, dass sicherheitsbezogenes Verhalten (Behavior) durch das Zusammenspiel von Wissen (Knowledge) und persönlicher Einstellung (Attitude) beeinflusst wird. Knowledge umfasst das Verständnis relevanter Sicherheitsregeln und -prozesse, Attitude beschreibt die individuelle Bewertung dieser Vorgaben, und Behavior bezieht sich auf das tatsächliche sicherheitsbezogene Handeln im Arbeitsalltag [36], [41].

Das KAB-Modell wurde ursprünglich in Bereichen wie Gesundheitsförderung [42], [43], [44] und Umweltverhalten [45], [46], [47], [48] eingesetzt und später erfolgreich auf den Bereich der Informationssicherheit übertragen [49], [50], [51]. Es bietet eine theoretisch fundierte Grundlage zur Erfassung von ISA als latente Dimension und bildet die konzeptionelle Basis sowohl für den HAIS-Q [36], [41] als auch für die entwickelte Kurzversion sHAIS-Q, indem Wissen, Einstellung und selbstberichtetes Verhalten systematisch erfasst werden.

**Identifikation und Schließung inhaltlicher Lücken im HAIS-Q**

Erster Schritt war es, bestehende inhaltliche Lücken im HAIS-Q zu identifizieren. Dazu wurden Ergebnisse aus Fokusgruppen mit Mitarbeitenden eines Universitätsklinikums

ausgewertet, in denen konkrete Hürden und Anreize im Umgang mit Informationssicherheit im Arbeitsalltag thematisiert wurden (sh. Abschnitt 0). Ergänzend wurde relevante Literatur analysiert [52]. Der Klinikkontext diente dabei als exemplarisches, vielschichtiges Umfeld, das durch seine berufliche Heterogenität besonders geeignet ist, um praxisrelevante Erweiterungen zu identifizieren. Auf dieser Grundlage wurden theoriegeleitet 39 neue Items entlang der KAB-Dimensionen formuliert, die gezielt inhaltliche Lücken des HAIS-Q adressieren. Die Items wurde so konzipiert, dass sie auch über den Klinikbereich hinaus generalisierbar einsetzbar bleibt. Im Anschluss wurden die Items durch ein systematisches Expertenrating bestehend aus 11 Experten und Expertinnen der Informationssicherheit hinsichtlich Klarheit und Relevanz bewertet und auf Basis des Feedbacks sprachlich wie inhaltlich überarbeitet.

**Sprachliche Übersetzung nach dem TRAPD-Verfahren**

Ziel war es, eine präzise und konzepttreue Version in Deutsch und Englisch zu erstellen, um die Vergleichbarkeit der Messung über Sprachgrenzen hinweg für internationale Studien zu ermöglichen, die statistisch mit dem Verfahren der Messinvarianz überprüft wurde. Für die sprachliche Umsetzung wurde der gesamte HAIS-Q einschließlich der neu entwickelten Zusatzitems übersetzt, sodass sie vollständig auf Deutsch und English verfügbar waren. Das Übersetzungsverfahren umfasst die Schritte Translation, Review, Adjudication, Pretesting und Documentation (TRAPD) und gilt als etablierter Standard für die Erstellung sprachlich und konzeptuell äquivalenter Fragebogenfassungen in der vergleichenden Sozialforschung ([53], [54]). Zunächst wurde eine parallele Übersetzung durch zwei unabhängige Fachübersetzerinnen angefertigt. Anschließend erfolgte eine strukturierte Überprüfung und Abstimmung durch ein Expertenteam mit Erfahrung in Fragebogenentwicklung und Informationssicherheit.

**Auswahlgesamtheit für die Validierungsstudie**

Zur Validierung des Instruments wurde eine international zusammengesetztes Auswahlgesamtheit verwendet. Insgesamt nahmen 1.182 berufstätige Personen aus dem Vereinigten Königreich (n = 581) sowie dem deutschsprachigen DACH-Raum (n = 601) an der Onlinebefragung teil. Die Erhebung erfolgte in deutscher und englischer Sprache über zwei unabhängige Access Panels (Prolific und Bilendi). Die Auswahlgesamtheit umfasste beschäftigte Personen mit einem durchschnittlichen Alter von M = 38,36 (Median = 36, Min = 18, Max = 77) sowie weibliche und männliche Personen mit einem Anteil von 46% bzw. 54%.

**Statistische Identifikation zwei weiterer Fokusgebiete im HAIS-Q**

Auf Basis der zusätzlich entwickelten Items wurden durch die Kombination explorativer Faktorenanalysen und inhaltsanalytischer Auswertungen zwei weitere thematische Schwerpunkte identifiziert: **präventive Sicherheitsorientierung** und **verantwortungsbewusster Informationsaustausch**. Diese Fokusbereiche wurden jeweils mit neun Items abgebildet und erweitern den ursprüngliche HAIS-Q um zwei weitere Fokusgebiete von ISA. Der gesamte Fragebogen mit der Erweiterung ist in Tabelle 17 einsehbar.

**Tabelle 17**: Items der deutschen psychometrischen Messung von Information Security Awareness des erweiterten HAIS-Q und der Kurzversion des sHAIS-Q

| Fokusbereiche | Unterkategorien | Wissen | Einstellung | Verhalten |
|---|---|---|---|---|
| **Passwortverwaltung** | Verwendung desselben Passworts | Es ist in Ordnung, ein Social-Media-Passwort auch für Arbeits-Accounts zu verwenden. | Es ist sicher, dasselbe Passwort für Social-Media-Konten und berufliche genutzte Accounts zu verwenden. | Für Social-Media-Konten und beruflich genutzte Accounts verwende ich jeweils ein eigenes Passwort. |
| | Teilen von Passwörtern | Ich darf mein Arbeitspasswort mit meinen Kolleginnen und Kollegen teilen. | Arbeitspasswörter sollte man nicht weitergeben. Auch dann nicht, wenn man von einem Kollegen oder einer Kollegin darum gebeten wird. | Ich teile meine Arbeitspasswörter mit meinen Kolleginnen und Kollegen. |
| | Verwendung eines starken Passworts | Für kurze Arbeitspasswörter muss man eine Kombination aus Buchstaben, Zahlen und Sonderzeichen verwenden. | Kurze Arbeitspasswörter, die nur aus Buchstaben bestehen, sind sicher genug. | Für kurze Arbeitspasswörter verwende ich eine Kombination aus Buchstaben, Zahlen und Sonderzeichen. |
| **E-Mail-Nutzung** | Klicken auf Links in E-Mails von bekannten Absendern | Ich darf jeden Link in einer E-Mail anklicken, wenn ich den Absender kenne. | Es ist stets sicher, Links in einer E-Mail anzuklicken, wenn ich den Absender kenne. | Ich klicke noch lange nicht auf jeden Link in einer E-Mail, nur weil ich den Absender kenne. |
| | Klicken auf Links in E-Mails von unbekannten Absendern | Ich darf nicht auf einen Link in einer E-Mail von einem unbekannten Absender klicken. | Es kann nicht viel passieren, wenn ich auf einen Link in einer E-Mail von einem unbekannten Absender klicke. | Wenn eine E-Mail eines unbekannten Absenders interessant erscheint, klicke ich einen Link darin an. |
| | Öffnen von Anhängen in E-Mails von unbekannten Absendern | Ich darf E-Mail-Anhänge von unbekannten Absendern öffnen. | Es ist riskant, einen E-Mail-Anhang von einem unbekannten Absender zu öffnen. | Ich öffne keine E-Mail-Anhänge, wenn ich den Absender nicht kenne. |
| **Internetnutzung** | Herunterladen von Dateien | Ich darf alle Dateien auf meinen Arbeitscomputer herunterladen, wenn sie | Es kann riskant sein, Dateien auf einen Arbeitscomputer herunterzuladen. | Auf meine Arbeitscomputer lade ich alle Dateien herunter, die mir helfen, |

| Fokusbereiche | Unterkategorien | Wissen | Einstellung | Verhalten |
|---|---|---|---|---|
| | | mir helfen, meine Arbeit zu erledigen. | | meine Arbeit zu erledigen. |
| | Zugriff auf dubiose Websites | Manche Webseiten sollte man bei der Arbeit besser nicht aufrufen. | Nur weil man bei der Arbeit auf eine Webseite zugreifen kann, bedeutet das noch lange nicht, dass diese auch sicher ist. | Wenn ich bei der Arbeit ins Internet gehe, besuche ich jede Webseite, die ich besuchen will. |
| | Eingabe von Informationen online | Ich darf auf jeder Webseite beliebige Informationen eingeben, wenn es mir hilft, meine Arbeit zu erledigen. | Wenn es mir hilft, meine Arbeit zu erledigen, spielt es keine Rolle, welche Informationen ich auf einer Webseite eingebe. | Ich bewerte, wie sicher Webseiten sind, bevor ich dort Informationen eingebe. |
| **Nutzung sozialer Medien** | Überprüfen der Privatsphäre-Einstellungen | Die Privatsphäre-Einstellungen von Social-Media-Accounts müssen regelmäßig überprüft werden. | Es ist sinnvoll, die Privatsphäre-Einstellungen von Social-Media-Accounts regelmäßig zu überprüfen. | Ich überprüfe die Privatsphäre-Einstellungen meiner Social-Media-Accounts nicht regelmäßig. |
| | Berücksichtigung von Konsequenzen | Ich kann nicht für etwas gekündigt werden, das ich in Social-Media veröffentliche. | In sozialen Medien kann ich bedenkenlos Dinge posten, die ich sonst nicht öffentlich sagen würde. | Ich veröffentliche nichts in Social-Media, bevor ich nicht die negativen Folgen bedacht habe. |
| | Posten über die Arbeit | In sozialen Medien kann ich über meine Arbeit posten, was ich will. | Es ist riskant, in Social-Media bestimmte Dinge über die eigene Arbeit zu posten. | In sozialen Medien poste ich über meine Arbeit, was ich will. |
| **Mobile Endgeräte** | Physische Sicherung mobiler Geräte | Wenn ich an einem öffentlichen Ort arbeite, muss ich mobile Geräte wie Laptop oder Tablet immer nah bei mir haben. | Wenn ich an einem öffentlichen Ort arbeite, ist es sicher, mobile Geräte wie Laptop oder Tablet für einen Moment unbeaufsichtigt zu lassen. | Wenn ich an einem öffentlichen Ort arbeite, lasse ich mobile Geräte wie Laptop oder Tablet unbeaufsichtigt. |
| | Senden sensibler Informationen über WLAN | Ich darf sensible Arbeitsdateien über ein öffentliches WLAN versenden. | Es ist riskant, sensible Arbeitsdateien über ein öffentliches WLAN zu versenden. | Ich versende sensible Arbeitsdateien über ein öffentliches WLAN. |
| | Schultersurfen **(sHAIS-Q)** | Wenn ich an einem vertraulichen Dokument arbeite, muss ich den Bildschirm von Laptop oder Tablet vor fremden Blicken schützen. | Es ist riskant, vertrauliche Dokumente auf mobilen Geräten wie Laptop oder Tablet zu öffnen, wenn Fremde den Bildschirm einsehen können. | Wenn ich an einem vertraulichen Dokument arbeite, stelle ich sicher, dass Fremde den Bildschirm des mobilen Geräts wie Laptop oder Tablet nicht einsehen können. |

| Fokusbereiche | Unterkategorien | Wissen | Einstellung | Verhalten |
|---|---|---|---|---|
| **Umgang mit Informationen** | Entsorgung sensibler Ausdrucke | Ausdrucke mit sensiblen Informationen können auf die gleiche Weise entsorgt werden wie Ausdrucke ohne sensible Informationen. | Ausdrucke mit sensiblen Informationen kann man bedenkenlos im Papierkorb entsorgen. | Wenn Ausdrucke mit sensiblen Informationen entsorgt werden müssen, sorge ich dafür, dass sie geschreddert oder vernichtet werden. |
| | Umgang mit entfernbaren Speichermedien | Wenn man einen USB-Stick an einem öffentlichen Ort finde, sollte man ihn nicht an einen Arbeitscomputer anschließen. | Wenn ich einen USB-Stick an einem öffentlichen Ort finde, kann nicht viel passieren, wenn ich ihn an einen Arbeitscomputer anschließe. | Ich würde einen USB-Stick, den ich an einem öffentlichen Ort finde, nicht an einen Arbeitscomputer anschließen. |
| | Zurücklassen sensibler Materialien **(sHAIS-Q)** | Ich darf Ausdrucke mit sensiblen Informationen auf dem Schreibtisch liegen lassen, wenn ich mich davon entferne. | Es ist riskant, Ausdrucke mit sensiblen Informationen unbeaufsichtigt auf dem Schreibtisch liegen zu lassen. | Ich lasse Ausdrucke mit sensiblen Informationen auf dem Schreibtisch liegen, wenn ich nicht vor Ort bin. |
| **Vorfallmeldung** | Verdächtiges Verhalten melden | Wenn ich beobachte, wie sich jemand auf der Arbeit verdächtig verhält, sollte ich das melden. | Es kann nichts Schlimmes passieren, wenn man verdächtiges Verhalten von anderen auf der Arbeit nicht weiter beachtet. | Wenn ich beobachten würde, wie sich jemand auf der Arbeit verdächtig verhält, würde ich etwas dagegen unternehmen. |
| | Ignorieren von Sicherheitsverhalten durch Kollegen | Ich darf ein mangelndes Sicherheitsverhalten meiner Kolleginnen und Kollegen nicht ignorieren. | Es macht nichts, wenn ich über mangelndes Sicherheitsverhalten meiner Kolleginnen und Kollegen hinwegsehe. | Falls ich bemerke, dass meine Kollegin oder mein Kollege die Sicherheitsvorschriften nicht beachtet, werde ich nichts dagegen unternehmen. |
| | Melden aller Vorfälle **(sHAIS-Q)** | Die Meldung von Sicherheitsvorfällen ist freiwillig. | Es ist riskant, Sicherheitsvorfälle zu ignorieren, auch wenn ich sie für unerheblich halte. | Wenn ich einen Sicherheitsvorfall bemerke, würde ich ihn melden. |
| **Präventive Sicherheitsorientierung** | Schulung & Sensibilisierung **(sHAIS-Q)** | Das Personal muss regelmäßig an Schulungen oder Fortbildungen in Sachen Informationssicherheit teilnehmen. | Es ist sinnvoll, dass das Personal regelmäßig an Schulungen oder Fortbildungen in Sachen Informationssicherheit teilnimmt. | Ich nehme regelmäßig an Schulungen oder Fortbildungen in Sachen Informationssicherheit teil. |
| | Richtlinienkenntnis **(sHAIS-Q)** | Das Personal muss sich regelmäßig über Vorschriften und Richtlinien der Organisation zur Informationssicherheit auf | Es ist angemessen, sich regelmäßig über Vorschriften und Richtlinien der Organisation zur | Ich informiere mich regelmäßig über die Vorschriften und Richtlinien zur Informationssicherheit in meiner Organisation. |

| Fokusbereiche | Unterkategorien | Wissen | Einstellung | Verhalten |
|---|---|---|---|---|
| | | dem Laufenden halten. | Informationssicherheit auf dem Laufenden zu halten. | |
| | Technische Sicherheitsmaßnahmen | Ich muss daran mitwirken, dass Sicherheitsupdates für Arbeitsgeräte regelmäßig durchgeführt werden. | Es ist wichtig, Sicherheitsupdates für Arbeitsgeräte regelmäßig durchzuführen. | Ich achte darauf, dass verfügbare Sicherheitsupdates auf meinen Arbeitsgeräten installiert werden. |
| **Verantwortungsbewusster Informationsaustausch** | Autorisierter Informationsaustausch | Ich darf mit anderen nur über vertraulichen Informationen sprechen, wenn eine Erlaubnis vorliegt. | Es ist wichtig, mit Unbefugten nicht über vertrauliche Informationen zu sprechen. | Es kommt vor, dass ich ohne Erlaubnis mit anderen über vertrauliche Informationen spreche. |
| | Lauschschutz **(sHAIS-Q)** | Wenn man über vertrauliche Informationen spricht, muss sichergestellt sein, dass Unbefugte nicht mithören können. | Es ist riskant, über vertrauliche Informationen zu sprechen, wenn Unbefugte mithören können. | Manchmal spreche ich über vertrauliche Informationen, obwohl andere mithören können. |
| | Verantwortungsbewusstsein bei Fehlverhalten **(sHAIS-Q)** | Die versehentliche Preisgabe sensibler Informationen an Unbefugte muss gemeldet werden. | Es ist wichtig zu melden, falls sensible Informationen versehentlich an Unbefugte preisgegeben werden. | Falls ich sensible Informationen versehentlich an Unbefugte preisgebe, werde ich dies melden. |

Anmerkung: Die englische Version ist im Maßnahmenkatalog unter www.medisa-projekt.de verfügbar. Die Kurzversion ist in der Spalte „Unterkategorien" mit der Kennzeichnung „sHAIS-Q" versehen. Die Items konnten auf eine vollständig numerisch verankerten 5-stufigen Likert-Skala mit den Ausprägungen von 1 = „Stimme überhaupt nicht" zu, 2 = „Stimme eher nicht zu", 3 = „teils, teils", 4 = „Stimme eher zu" und 5 = „Stimme voll und ganz zu" bewertet werden.

### Anpassungsgüte und Faktorenladungen des HAIS-Q und sHAIS-Q

Die Ergebnisse der Modellfit-Indices für die verschiedenen Versionen des HAIS-Q mit DWLS (Diagonally Weighted Least Squares)-Schätzung zeigten durchweg sehr gute Anpassungsgüten. Der erweiterte HAIS-Q mit 81 Items weist in der deutschen Version einen CFI (Comparative Fit Index) von 0,962 und einen RMSEA (Root Mean Square Error of Approximation) von 0,07 (90%-Konfidenzintervall: 0,069–0,072) auf. Diese Werte deuten auf ein gutes Modell hin, auch wenn der RMSEA leicht oberhalb der optimalen Schwelle liegt. Die englische Version zeigt mit einem CFI von 0,976, einem RMSEA von 0,059 (CI: 0,058–0,061) und einem SRMR (Standardized Root Mean Square Residual) von 0,071 ein exzellentes Fit. Besonders bemerkenswert ist die Leistung der Kurzform (sHAIS-Q) mit nur 21 Items: In der deutschen Version erreicht sie trotz der starken Reduktion einen sehr hohen CFI von 0,980 und einen akzeptablen RMSEA von 0,085 (CI: 0,080–0,090). Die englische Kurzversion übertrifft sogar diese Werte mit einem exzellenten CFI von 0,986, einem RMSEA von 0,076 (CI: 0,070–0,081) und einem niedrigen SRMR von 0,067.

Die Analyse der standardisierten Faktorladungen für die deutsche und englische Version ergab insgesamt zufriedenstellende Werte. In der erweiterten Version des HAIS-Q lagen die durchschnittlichen Faktorladungen bei 0,64 (deutsch) bzw. 0,65 (englisch). Zwei Verhaltensitems unterschritten die häufig genannte Mindestgrenze von 0,40 [55] („Ich überprüfe die Privatsphäre-Einstellungen meiner Social-Media-Accounts nicht regelmäßig.", Faktorladung = 0,27; „Ich würde einen USB-Stick, den ich an einem öffentlichen Ort finde, nicht an einen Arbeitscomputer anschließen.", standardisierte Faktorladung = 0,36), blieben jedoch im Modell, da sie Bestandteil des originalen HAIS-Q sind. Für die Kurzversion (sHAIS-Q) lagen die durchschnittlichen Faktorladungen in beiden Sprachfassungen bei 0,75, was auf eine sehr gute Indikatorqualität hinweist.

**Statistische Identifikation der Items des sHAIS-Q**

Da der ursprüngliche HAIS-Q mit 63 Items bereits sehr umfangreich ist und im Rahmen dieser Studie zusätzlich 18 neue Items zu den Themen präventive Sicherheitsorientierung und verantwortungsbewusste Informationsweitergabe entwickelt wurden, umfasste der vollständige Itempool insgesamt 81 Items. Auf Basis der Validierungsdaten aus der Prolific Stichprobe wurde daraus eine ökonomische Kurzversion abgeleitet, die den Umfang des ursprünglichen HAIS-Q um etwa zwei Drittel reduziert. Die resultierende Kurzskala umfasst 21 Items, jeweils sieben pro KAB-Dimension, ausgewählt anhand der höchsten mittleren Faktorladungen. Ein Item Triplet wurde aus inhaltlichen Gründen ausgetauscht. Insgesamt stammen 16 der 21 Items aus eigener Entwicklung. Die Items 21 Items des sHAIS-Q sind in der Tabelle 17 markiert.

**Messinvarianz**

Die Überprüfung der Messinvarianz zwischen den englischen und deutschen Stichproben (sh. Tabelle 18) ergab eine akzeptable Modellstabilität sowohl für sHAIS-Q als auch für die HAIS-Q-Skalen. Für beide Instrumente wurde schrittweise auf Konfigurations-, Schwellenwert-, metrische (Schwellenwerte und Ladungen gleichgesetzt) sowie skalare Invarianz (Schwellenwerte, Ladungen und Interzepte gleichgesetzt) getestet, basierend auf einem etablierten Vorgehen [56]. In allen Modellen mit DWLS-Schätzung blieben die Veränderungen in den Fit-Indizes innerhalb der empfohlenen Grenzwerte ($\Delta CFI \geq -0{,}01$; $\Delta RMSEA \leq 0{,}015$; [57]) was skalare Invarianz unterstützt. Die Skalen der sHAIS-Q und des HAIS-Q zeigten über alle Invarianzstufen hinweg besonders stabile Modellanpassungen mit minimalen Veränderungen in CFI und RMSEA. Die Etablierung skalarer Invarianz ermöglicht einen sinnvollen Vergleich von Mittelwerten latenter Konstrukte zwischen Sprachgruppen und legt damit die Grundlage für kulturvergleichende Forschung [58].

**Tabelle 18**: Messinvarianz zwischen der deutschen und englischen Version des HAIS-Q und sHAIS-Q

| Model und Restriktionen | $\chi^2$ | df | CFI | RMSEA | $\Delta\chi^2$ | Δdf | ΔCFI | ΔRMSEA |
|---|---|---|---|---|---|---|---|---|
| **HAIS-Q** | | | | | | | | |
| Configural Invariance | 20459,39 | 5844 | 0,969 | 0,065 | | | | |
| Thresholds | 20541,63 | 5997 | 0,969 | 0,064 | 82,24 | 153 | 0,000 | -0,001 |
| Thresholds and loadings | 20752,37 | 6072 | 0,969 | 0,064 | 210,74 | 75 | 0,000 | 0,000 |
| Thresholds, loadings, and intercepts | 21875,01 | 6147 | 0,967 | 0,066 | 1122,64 | 75 | -0,002 | 0,002 |
| **sHAIS-Q** | | | | | | | | |
| Configural Invariance | 1790,08 | 372 | 0,983 | 0,080 | | | | |
| Thresholds c | 1811,08 | 413 | 0,984 | 0,076 | 21,00 | 41 | 0,000 | -0,005 |
| Thresholds and loadings | 1841,88 | 431 | 0,983 | 0,074 | 30,80 | 18 | 0,000 | -0,001 |
| Thresholds, loadings, and intercepts | 1897,43 | 449 | 0,983 | 0,074 | 55,55 | 18 | 0,000 | -0,001 |

Anmerkung: ***p ≤ ,001, **p ≤ ,01, *p ≤ ,05. Englisch n = 581 aus UK und deutsch umfasst n = 601 aus der DACH-Region.

### Reliabilitäten und Konvergente Validität

Die Analyse der konvergenten Validität zeigt insgesamt sehr gute Ergebnisse für beide Sprachversionen (Deutsch und Englisch) des HAIS-Q seiner Kurzform im sHAIS-Q (sh. Tabelle 19). Die Korrelationen zwischen den entsprechenden Subskalen der Lang- und Kurzform sind durchweg hoch. Besonders deutlich wird dies bei den analogen Subskalen Knowledge, Attitude und Behavior, die sowohl in der deutschen als auch in der englischen Version zwischen HAIS-Q und sHAIS-Q stark korrelieren (r = 0,85 bis r = 0,89), was auf eine enge inhaltliche Übereinstimmung hinweist.

In Bezug auf die externen Validierungskriterien zeigen die Korrelationen mit der Security Behavior Intentions Scale (SeBIS) [59] und der Simplified Information Security Awareness Scale (SISA) [60] ein konsistentes Bild über beide Sprachräume hinweg. Die sHAIS-Q-Subskalen korrelieren mit den SeBIS- und SISA-Skalen in einem vergleichbaren Ausmaß wie die Langform, was für eine gleichwertige konvergente Validität spricht. Dabei zeigt sich erwartungsgemäß, dass SeBIS, eine Skala zur Erfassung sicherheitsbezogener Verhaltensintentionen, insbesondere mit den Verhaltensdimensionen des HAIS-Q und sHAIS-Q am höchsten korreliert (zum Beispiel r = .33 bis .52 in den deutschen Daten; r = .29 bis .45 in den englischen Daten). Dies unterstützt die theoretische Annahme, dass Verhaltensintentionen und berichtetes Sicherheitsverhalten besonders eng verknüpft sind.

Die Reliabilitätskennwerte der Skalen, angegeben als McDonald's ω und berechnet auf Basis polychorischer Korrelationen, sind durchweg als sehr gut zu bewerten. Die HAIS-

Q-Skalen erreichen Werte zwischen ω = .94 und .96, während auch die sHAIS-Q-Kurzform reliabel ist mit Werten zwischen ω = .87 und .92.

**Tabelle 19:** Reliabilitäten und Konvergente Korrelationen mit HAIS-Q und sHAIS-Q

| Variable | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Deutsch (DACH)* | | | | | | | | | | | |
| 1. HAIS-Q Knowledge | *(0,94)* | | | | | | | | | | |
| 2. HAIS-Q Attitude | 0,68 | *(0,96)* | | | | | | | | | |
| 3. HAIS-Q Behavior | 0,64 | 0,74 | *(0,94)* | | | | | | | | |
| 4. sHAIS-Q Knowledge | 0,88 | 0,57 | 0,58 | *(0,88)* | | | | | | | |
| 5. sHAIS-Q Attitude | 0,57 | 0,85 | 0,68 | 0,56 | *(0,91)* | | | | | | |
| 6. sHAIS-Q Behavior | 0,52 | 0,58 | 0,87 | 0,56 | 0,63 | *(0,89)* | | | | | |
| 7. SeBIS Device Securement | 0,23 | 0,26 | 0,34 | 0,20 | 0,27 | 0,33 | *(0,73)* | | | | |
| 8. SeBIS Password Generation | 0,26 | 0,33 | 0,52 | 0,23 | 0,33 | 0,47 | 0,33 | *(0,78)* | | | |
| 9. SeBIS (Proactive Awareness) | 0,30 | 0,39 | 0,51 | 0,22 | 0,30 | 0,41 | 0,26 | 0,44 | *(0,69)* | | |
| 10. SeBIS (Updating) | 0,24 | 0,34 | 0,46 | 0,26 | 0,35 | 0,44 | 0,26 | 0,47 | 0,32 | *(0,76)* | |
| 11. SISA | 0,45 | 0,56 | 0,64 | 0,43 | 0,52 | 0,57 | 0,27 | 0,41 | 0,43 | 0,42 | *(0,76)* |
| | | | | | | | | | | | |
| *Englisch (UK)* | | | | | | | | | | | |
| 1. HAIS-Q Knowledge | *(0,95)* | | | | | | | | | | |
| 2. HAIS-Q Attitude | 0,70 | *(0,96)* | | | | | | | | | |
| 3. HAIS-Q Behavior | 0,71 | 0,74 | *(0,94)* | | | | | | | | |
| 4. sHAIS-Q Knowledge | 0,87 | 0,64 | 0,64 | *(0,89)* | | | | | | | |
| 5. sHAIS-Q Attitude | 0,63 | 0,87 | 0,66 | 0,64 | *(0,92)* | | | | | | |
| 6. sHAIS-Q Behavior | 0,60 | 0,63 | 0,89 | 0,63 | 0,65 | *(0,87)* | | | | | |
| 7. SeBIS Device Securement | 0,25 | 0,21 | 0,35 | 0,25 | 0,21 | 0,33 | *(0,68)* | | | | |
| 8. SeBIS Password Generation | 0,24 | 0,25 | 0,45 | 0,18 | 0,23 | 0,41 | 0,39 | *(0,81)* | | | |
| 9. SeBIS (Proactive Awareness) | 0,20 | 0,26 | 0,35 | 0,16 | 0,19 | 0,29 | 0,22 | 0,37 | *(0,67)* | | |
| 10. SeBIS (Updating) | 0,24 | 0,29 | 0,44 | 0,22 | 0,29 | 0,42 | 0,34 | 0,54 | 0,26 | *(0,79)* | |
| 11. SISA | 0,39 | 0,48 | 0,58 | 0,35 | 0,43 | 0,53 | 0,28 | 0,37 | 0,28 | 0,40 | *(0,74)* |

Anmerkung: Dargestellt sind Pearsons Korrelationen auf Basis von Mittelwerten über die Subskalen. Alle Korrelationen weisen nach einer Holm Korrektur einen p-Wert < .001 auf. HAIS-Q = Human Aspects of Information Security Questionnaire, SeBIS = Security Behavior Intenions Scale, SISA = Simplified Information Security Awareness Scale. SeBIS und SISA wurden für die Validierungsstudie mit dem TRAPD-Verfahren auf Deutsch übersetzt und zeigten ebenfalls skalare Messinvarianz (Ergebnisse auf Anfrage).

### Diskriminanten Validität

Zur Beurteilung der Diskriminanten Validität in Bezug auf organisationale Datenschutzbedenken wurden die Subskalen des Concerns for Information Privacy (CFIP) mit den Dimensionen des HAIS-Q und sHAIS-Q verglichen. Die CFIP-Skala umfasst vier Dimensionen (Collection, Errors, Unauthorized Secondary Use und Improper Access). In allen Fällen lagen die HTMT-Werte deutlich unter dem etablierten Schwellenwert von 0.85 (min. = 0,07 bis max. = 0,59), was auf eine klare Abgrenzung der Konstrukte hindeutet. Dabei zeigten sich durchweg die höchsten Überschneidungen mit der CFIP-Dimension

Improper Access, die sowohl mit den HAIS-Q- als auch den sHAIS-Q-Subskalen „Attitude“ und „Behavior“ HTMT-Werte von 0,41 bis 0,59 erreichte, die aber immer noch im moderaten Bereich liegen. Diese Zusammenhänge sind theoretisch nachvollziehbar, da Improper Access auf die Sensibilität gegenüber unbefugtem Zugriff auf persönliche Daten zielt und somit konzeptuell mit sicherheitsbezogenen Einstellungen und Verhaltensweisen verwandt ist. Insgesamt zeigen die Ergebnisse, dass HAIS-Q als auch sHAIS-Q eigenständige Konstrukte erfassen, die sich klar vom Konzept Datenschutzbedenken unterscheiden lassen.

**Zusammenfassung und Fazit**

Der sHAIS-Q zeigt eine hohe Übereinstimmung mit dem erweiterten HAIS-Q und weist in beiden Sprachversionen gute Werte hinsichtlich Anpassungsgüte, konvergenter und diskriminanter Validität sowie Reliabilität auf. Die skalare Invarianz ermöglicht einen zuverlässigen Vergleich latenter Mittelwerte zwischen der deutschen und der englischen Version und schafft damit eine Grundlage für kulturvergleichende Forschung.
Aufgrund seiner konsistenten Ergebnisse und kompakten Form stellt der sHAIS-Q eine valide und praktikable Alternative zur Langversion dar. Zudem erlaubt er die gezielte Erfassung einzelner Dimensionen wie Wissen, Einstellung oder selbstberichtetes Verhalten. Bereits sieben Items reichen aus, um die jeweiligen Konstrukte valide abzubilden. Der sHAIS-Q eignet sich damit besonders für den Einsatz in medizinischen Einrichtungen.

## Erhebung von Meinungsbildern: Quantitative Analyse von Informationssicherheitsbewusstsein im Zusammenhang zu Hürden und Anreizen in einer Universitätsklinik

Aufbauend auf qualitativen Erkenntnissen aus Experten- und Expertinnen-Interviews (sh. Kapitel 5.1) und Fokusgruppen mit Mitarbeitenden (sh. Kapitel 5.2), in denen unter anderem Hürden, Anreize sowie organisationale Rahmenbedingungen für ISA diskutiert wurden, sollte die vorliegende quantitative Befragung eine empirische Fundierung dieser Eindrücke leisten und deren Generalisierbarkeit in einer anderen Universitätsklinik überprüfen.
Zu diesem Zweck wurde eine Online-Erhebung in einer deutschen Universitätsklinik mit rund 10.000 Beschäftigten durchgeführt. Ziel der Untersuchung war es, ein differenziertes Meinungsbild zu mentalen Modellen und Einflussfaktoren im Zusammenhang mit Informationssicherheit zu gewinnen:

- Im Mittelpunkt stand die Frage, welche organisatorischen und arbeitsprozessbezogenen und individuellen Hürden und Anreize das sicherheitsbezogene Wissen, die Einstellungen und das Verhalten des Personals beeinflussen.

- Ergänzend wurde der neu entwickelte Fragebogen sHAIS-Q im klinischen Anwendungskontext erprobt, um seine Praxistauglichkeit und psychometrische Qualität zu prüfen.

- Zudem wurde analysiert, ob sich Hinweise auf gruppenspezifische Unterschiede in Bezug auf das Informationssicherheitsbewusstsein identifizieren lassen.

Insgesamt tragen die Ergebnisse dazu bei, die qualitativen Befunde systematisch zu ergänzen und bilden eine evidenzbasierte Grundlage für die Entwicklung passgenauer Awareness-Materialien in medizinischen Einrichtungen.

**Teilnehmende**

Auf Basis einer Einladung der Stabstelle für Informationssicherheit, nahmen an der Befragung insgesamt **579 beschäftigte** Personen teil. Dabei ergab sich einen Rücklaufquote von 6,6%. Eine Inferenzierbarkeit auf die gesamte Klink muss mit Vorsicht interpretiert werden, da es sich nicht um eine Stichprobe, sondern um eine Selbstselektion von Teilnehmenden handelt. Etwa die Hälfte der Befragten (47 %) war im unmittelbaren Gesundheitsbereich tätig, darunter ärztlicher Dienst, Pflege-, Funktions- und medizinisch-technische Dienste. Die übrigen 53 % gehörten zu nicht-medizinischen Bereichen wie Forschung, Verwaltung, IT, Technik oder unterstützenden Diensten (sh. Tabelle 20). Hiervon ordneten sich 58,9% dem weiblichen und 27,5% dem männlichen Geschlecht zu, 13,6% haben keine Angabe zum Geschlecht hinterlassen.

**Tabelle 20**: Verteilung der Teilnehmenden nach Personalgruppen

| **Personalgruppe** | **Anzahl** | **Anteil (%)** |
|---|---|---|
| Ärztlicher Dienst | 55 | 9,5 |
| Pflege & Funktionsdienst | 98 | 16,9 |
| Medizinisch-technischer Dienst | 115 | 19,9 |
| Forschung | 66 | 11,4 |
| Verwaltung | 157 | 27,1 |
| IT | 40 | 6,9 |
| Sonstige | 37 | 6,4 |
| Unbekannte Personalgruppe | 11 | 1,9 |
| **Gesamt** | **579** | **100** |

**Praktikabilität: Beantwortungszeiten, faktorielle Validität und Reliabilitäten**

Zur Einschätzung der **Bearbeitungszeit** wurden die einzelnen Skalenbereiche separat analysiert. Die Ergebnisse zeigen, dass der zeitliche Aufwand insgesamt gering ist und somit eine Anwendung des Instruments auch im klinischen Alltag realistisch erscheint. Für den *Wissen* lag die durchschnittliche Bearbeitungszeit bei *1,11 Minuten*, mit einem Median von 1,05 Minuten. Die schnellste Bearbeitung betrug rund 23 Sekunden, die längste etwa 2,39 Minuten. Die Skala zur *Einstellung* gegenüber Informationssicherheit wies eine mittlere Bearbeitungszeit von *0,84 Minuten* auf (Median: 0,79 Minuten). Die Zeiten reichten von 15 Sekunden bis zu 1,88 Minuten. Der Bereich zum sicherheitsbezogenen *Verhalten* wurde im Durchschnitt in *0,82 Minuten* bearbeitet (Median: 0,78 Minuten), mit einer Spannweite von 13 Sekunden bis 1,70 Minuten.

Zur Prüfung der **faktoriellen Validität** des sHAIS-Q wurde eine konfirmatorische Faktorenanalyse mit DWLS-Schätzung durchgeführt. Die Ergebnisse zeigen eine insgesamt gute Modellanpassung an die empirischen Daten. Die globalen Fit-Indizes bestätigen dies: Der CFI liegt bei 0,965 und der RMSEA bei 0,087 (90 %-KI: 0,082–0,092), was auf eine akzeptable Modellpassung hinweist. Der SRMR beträgt 0,087 und liegt damit ebenfalls im akzeptablen Bereich. Die standardisierten Faktorladungen für alle Items in den drei latenten Dimensionen (Wissen, Einstellung und Verhalten) liegen zwischen 0,46 und 0,84 und im Schnitt bei 0,69, was auf eine durchweg gute Indikatorvalidität hinweist. Alle Ladungen sind signifikant ($p < .001$). Damit lässt sich die zugrundeliegende theoretische Dreifaktorenstruktur des sHAIS-Q empirisch gut abbilden. Insgesamt stützen die Ergebnisse die faktorielle Validität des sHAIS-Q und belegen, dass das Instrument valide latente Konstrukte zur Erfassung des Informationssicherheitsbewusstseins im klinischen Kontext misst.

Ebenfalls zeigen sich sehr gute **Reliabilitätswerte** für alle drei Skalenbereiche des sHAIS-Q, berechnet auf Basis von McDonald's ω (polychorisch): Für den Wissensbereich beträgt die Reliabilität 0,80, für die Einstellungsskala 0,91 und für das sicherheitsbezogene Verhalten 0,83. Diese Ergebnisse sprechen für eine hohe interne Konsistenz der Skalen.

Insgesamt sprechen die Ergebnisse für eine **hohe Praktikabilität des sHAIS-Q**. Alle drei Subskalen lassen sich in kurzer Zeit (in etwa 3 Min.) ausfüllen und zeigen im Anwendungskontext einer Universitätsklinik eine adäquate faktorielle Validität sowie sehr gute interne Konsistenzen. Damit eignet sich das Instrument auch für den Einsatz im zeitlich stark beanspruchten Umfeld medizinischer Einrichtungen und stellt eine effiziente Möglichkeit zur Erfassung des kognitiven Informationssicherheitsbewusstseins dar.

**Unterschiede in ISA nach Personalgruppen**

Eine Regressionsanalyse (sh. Tabelle 21) untersuchte ISA differenziert nach den Unterdimensionen Wissen, Einstellung und selbstberichtetes Verhalten in Abhängigkeit von der Personalgruppe und unter Kontrolle des Geschlechts. Zunächst wird deutlich, dass ISA über alle Dimensionen hinweg, sich auf einem hohen Niveau befindet. Es zeigt sich zudem, dass bei Wissen und Einstellung keine signifikanten Unterschiede zwischen den Personalgruppen oder nach Geschlecht vorliegen. Lediglich die IT weist etwas höheres Wissen im Vergleich zur Verwaltung auf und weibliche Personen waren mit marginal höheren Einstellungswerten im Vergleich zu männlichen Kollegen assoziiert, allerdings auf einem 10 %-Signifikanzniveau. Beim Verhalten zeigten sich die größten Unterschiede in ISA: Ärztlicher Dienst, Pflege- und Funktionsdienst, Medizinisch-Technischer Dienst sowie die Forschung weisen im Vergleich zur Verwaltung signifikant niedrigere ISA-Verhaltenswerte auf. Lediglich die IT zeigt höhere Werte, die aber ebenfalls nur auf einem 10 %-Signifikanzniveau.

Da sich die Personalgruppen in Bezug auf Wissen und Einstellung zur Informationssicherheit nicht signifikant unterscheiden, deutet dies darauf hin, dass weniger die bewusste Haltung oder Kenntnislage, sondern vielmehr die arbeitsplatzbezogene Einbettung und Praxisanforderungen für das sicherheitsbezogene Verhalten von Bedeutung sind.

**Tabelle 21**: Regressionsanalyse für eine Differenzierung von Informationssicherheitsbewusstsein nach Personalgruppen unter Kontrolle von Geschlecht

| **sHAIS-Q** | **Wissen** | **Einstellung** | **Verhalten** |
|---|---|---|---|
| Interzept | 4,59*** | 4,60*** | 4,23*** |
| | 0,05 | 0,05 | 0,07 |
| Ärztlicher Dienst | -0.10 | -0,07 | -0,29** |
| | 0,08 | 0,08 | 0,10 |
| Pflege- & Funktionsdienst | -0,10 | -0,06 | -0,18* |
| | 0,06 | 0,06 | 0,08 |
| Med.-techn. Dienst | -0,03 | -0,13 | -0,25** |
| | 0,06 | 0,06 | 0,08 |
| Forschung | 0,00 | -0,07 | -0,20* |
| | 0,07 | 0,07 | 0,10 |
| IT | 0,17† | 0,13 | 0,21† |
| | 0,09 | 0,09 | 0,12 |
| Sonstige Personalgruppe | -0,11 | -0,01 | -0,18 |
| | 0,09 | 0,09 | 0,12 |
| Unbekannte Personalgruppe | 0,09 | 0,02 | -0,20 |
| | 0,15 | 0,15 | 0,21 |
| Weiblich | 0,02 | 0,09 | 0,04 |
| | 0,05 | 0,05 | 0,07 |

| sHAIS-Q | Wissen | Einstellung | Verhalten |
|---|---|---|---|
| Geschlecht unbekannt | 0,00 | 0,05† | 0,00 |
| | 0,07 | 0,07 | 0,09 |
| | | | |
| $R^2$ | 0,021 | 0,019 | 0,043 |
| Angepasstes $R^2$ | 0,006 | 0,004 | 0,027 |
| F-Test (df1, df2) | 1,387 (9, 569) | 1,254 (9, 569) | 2,809** (9, 569) |
| n | 579 | 579 | 579 |

Anmerkung: Signifikanzniveaus: ***p < 0,001; **p < 0,01; *p < 0,05; †p < 0,10. Der Interzept bezieht sich auf die Referenzkategorie „Verwaltung" bei der Personalgruppe und „männlich" beim Geschlecht. Alle Effektgrößen sind unstandardisierte Regressionskoeffizienten; Standardfehler stehen jeweils darunter. Die ISA-Subdimensionen wurden auf Basis von Mittelwerten berechnet.

### Quantitativer Zusammenhang von ISA zu Hürden und Anreizen

Tabelle 22 zeigt eine Korrelationsmatrix der zentralen ISA-Dimensionen Wissen, Einstellung und Verhalten sowie deren Zusammenhänge mit verschiedenen organisatorischen, arbeitsprozessbezogenen und individuellen Hürden und Anreizen (An dieser Stelle sei darauf hingewiesen, dass es sich um bivariate Zusammenhänge ohne Kontrolle zusätzlicher Drittvariablen handelt und keine kausalen Wirkungsrichtungen abgeleitet werden können. Die Ergebnisse sind daher als rein assoziativ zu verstehen).

**Tabelle 22:** Pearson Korrelationen zwischen den latenten Dimensionen des Informationssicherheitsbewusstseins (Wissen, Einstellung, Verhalten) und ausgewählten Hürden und Anreizen

| Variable | 1 | 2 | 3 |
|---|---|---|---|
| 1. ISA-Wissen | *0,80* | | |
| 2. ISA-Einstellung | 0,89*** | *0,91* | |
| 3. ISA-Verhalten | 0,77*** | 0,84*** | *0,83* |
| *Organisatorische Rahmenbedingungen* | | | |
| Top-Management Commitment für ISR | 0,47*** | 0,41*** | 0,50*** |
| Verfügbarkeit von ISR | 0,50*** | 0,46*** | 0,62*** |
| Unterstützung Einhaltung von ISR | 0,52*** | 0,47*** | 0,64*** |
| ISR-Sanktionen | 0,37*** | 0,37*** | 0,39*** |
| Technische Hürden | -0,05* | -0,09*** | -0,18*** |
| *Arbeitsprozesse* | | | |
| ISR als Arbeitshindernis | -0,25*** | -0,35*** | -0,35*** |
| ISR-Nachlässigkeit | -0,39*** | -0,46*** | -0,52*** |
| Arbeitslast und Zeitdruck | 0,08** | 0,07*** | 0,04* |
| Informelle Schattenprozesse konträr zu ISR | -0,28*** | -0,35*** | -0,39*** |
| *Individuelle Faktoren* | | | |

| Variable | 1 | 2 | 3 |
|---|---|---|---|
| Selbstwirksamkeit | 0,48*** | 0,38*** | 0,56*** |
| EDV-Kenntnisse | 0,12*** | -0,09*** | -0,05* |

Anmerkung: Signifikanzniveaus: ***p < 0,001; **p < 0,01; *p < 0,05. Reliabilitäten (McDonald's ω auf Basis polychorischer Korrelationen) sind in der Diagonale Kursiv dargestellt. Reliabilitäten der weiteren latenten Variablen liegt bei 0,79 bis 0,92. ISR = Informationssicherheits-Richtlinie. EDV = Elektronische Datenverarbeitung.

Die ISA-Dimensionen selbst korrelieren sehr stark miteinander: So zeigt sich ein besonders enger Zusammenhang zwischen Wissen und Einstellung (r = 0,89***), sowie zwischen Einstellung und Verhalten (r = 0,84***). Auch Wissen und Verhalten hängen deutlich zusammen (r = 0,77***). Diese engen Zusammenhänge bestätigen grundlegende Annahmen aus der Awareness-Forschung, wonach Wissen und Einstellungen zentrale Voraussetzungen für sicherheitskonformes Verhalten darstellen [41]. In den Experten- und Expertinnen-Interviews (Kapitel 5.1) wurde ebenfalls betont, dass der Aufbau eines Grundverständnisses und kontinuierliche Sensibilisierung entscheidend ist, was sich hier auch quantitativ widerspiegelt.

In Bezug auf organisatorische Rahmenbedingungen zeigt sich, dass das Commitment des Top-Managements, dessen Verfügbarkeit sowie die Unterstützung bei der Einhaltung von Informationssicherheitsrichtlinien (ISR) positiv mit allen drei ISA-Dimensionen zusammenhängen. Dies unterstreicht die in den Interviews und Workshops (vgl. Kapitel 5.1 und 5.2) geäußerte Kritik an der mangelnden Unterstützung durch die Leitungsebene, dem fehlenden Zugang zu klaren Strukturen und gut auffindbaren Materialien, Verwendung generischer Schulungsinhalte mit geringem Praxisbezug sowie der häufig unzureichenden Einbindung des betroffenen Personals bei der Umsetzung von Informationssicherheits-Maßnahmen.

In Bezug auf arbeitsprozessbezogene Aspekte wie die Nachlässigkeit im Umgang mit Informationssicherheitsrichtlinien weist mit einem Korrelationswert von r = –0,52*** die stärkste negative Verbindung zu ISA-Verhalten auf. Dies lässt darauf schließen, dass bewusstes oder unbewusstes Abweichen von Regeln eine zentrale Barriere für Informationssicherheit im klinischen Alltag darstellt. In den Experten- und Expertinnen-Interviews wird auf Überforderung, Unachtsamkeit und das wiederholte Ignorieren von Warnhinweisen bei Phishing hingewiesen. Auch in den Fokusgruppen berichten Teilnehmende, dass Sicherheitsvorgaben aufgrund von unzureichender Wahrnehmung und Aufmerksamkeit nicht beachtet werden.

Das Erleben von Informationssicherheitsrichtlinien als hinderlich korreliert negativ mit Wissen (r = –0,25***), Einstellung (r = –0,35***) und Verhalten (r = –0,35***). Diese Zusammenhänge finden sich auch in den Fokusgruppen wieder, indem Mitarbeitende

Sicherheitsanforderungen als zusätzlichen Aufwand empfinden, der schwer mit der unmittelbaren Patientenversorgung zu vereinbaren ist.

Arbeitslast und Zeitdruck zeigen nur sehr geringe positive Zusammenhänge mit den ISA-Dimensionen (Wissen: r = 0,08**, Einstellung: r = 0,07***, Verhalten: r = 0,04*). Diese statistischen Befunde wirken auf den ersten Blick kontraintuitiv, da Arbeitsüberlastung häufig als Hürde für sicherheitskonformes Verhalten beschrieben wird. In den Fokusgruppen wurde deutlich, dass Multitasking, hoher Zeitdruck sowie die Notwendigkeit ständiger Erreichbarkeit dazu führen, dass Informationssicherheitsmaßnahmen vernachlässigt wird. Es kann aber auch abgeleitet werden, dass hohe Belastung im Arbeitsalltag nicht der entscheidende Hinderungsgrund für sicherheitskonformes Verhalten ist und dass Mitarbeitende trotz oder gerade wegen des hohen Zeitdrucks ein gewisses Problembewusstsein für Informationssicherheit bewahren. Möglicherweise schärft die Erfahrung eines hektischen, störanfälligen Arbeitsumfelds das Bewusstsein für potenzielle Risiken, auch wenn die konkrete Umsetzung von Maßnahmen unter diesen Bedingungen erschwert ist.

Auch informelle Schattenprozesse, die den offiziellen Sicherheitsvorgaben widersprechen, zeigen einen signifikant negativen Zusammenhang mit ISA. Solche abweichenden Prozesse entstehen häufig aus praktischen Zwängen, etwa um Arbeitsabläufe effizienter zu gestalten. Eine Studie zeigt, dass beispielsweise das Teilen von Passwörtern oder das Umgehen von Authentifizierungsprozessen verbreitet ist [52]. Diese Muster stehen in einem deutlichen Widerspruch zu den intendierten Sicherheitsmaßnahmen und untergraben deren Wirksamkeit.

Die Variable Selbstwirksamkeit zeigt deutliche positive Korrelationen mit allen ISA-Dimensionen, insbesondere mit Verhalten (r = 0,56***). Dies steht in engem Zusammenhang mit qualitativen Aussagen zur Bedeutung des „Faktor Mensch“ als Chance (s Kapitel 5.1): Geschulte und motivierte Mitarbeitende, die ihre Kompetenzen aktiv erleben und einsetzen können, sind eine wichtige Ressource für Sicherheitskultur und -verhalten.

Ein weiterer Faktor ist die Wahrnehmung von Sanktionen im Zusammenhang mit Verstößen gegen Informationssicherheitsrichtlinien (Wissen: r = 0,37***, Einstellung: r = 0,37***, Verhalten: r = 0,39***). Diese Ergebnisse legen nahe, dass Sanktionen eine regulierende Funktion erfüllen können. Es ist aber davon auszugehen, dass Mitarbeitende nicht primär aufgrund potenzieller Strafen sicherheitsgerecht handeln, sondern eher dann, wenn sie sich unterstützt fühlen, Informationen zugänglich sind und sie sich in ihrer Rolle wirksam erleben. Auch in den Fokusgruppen fanden Sanktionen keine besondere Betonung.

Technische Hürden zeigen nur schwache negative Zusammenhänge mit ISA-Verhalten (r = –0,18***), Einstellung (r = –0,09***) und Wissen (r = –0,05*), was darauf hinweist,

dass technische Probleme zwar vorhanden sind, aber keine zentrale Erklärung für mangelnde Awareness darstellen. Interviews und Fokusgruppen bestätigen, dass veraltete Systeme, lange Ladezeiten und fehlende Schnittstellen den Arbeitsalltag erschweren, jedoch meist im Zusammenspiel mit organisatorischen Schwächen wirken. Auch EDV-Kenntnisse erklären ISA nur begrenzt: Während sie leicht positiv mit Wissen korrelieren (r = 0,12***), zeigen sich negative Zusammenhänge mit Einstellung (r = –0,09***) und Verhalten (r = –0,05*). Das deutet darauf hin, dass technisches Know-how im Vergleich nicht der entscheidende Faktor für ISA ist.

**Fazit und Implikationen**

Die Ergebnisse der quantitativen Befragung liefern empirische Einblicke in das Informationssicherheitsbewusstsein innerhalb einer großen Universitätsklinik. Der eingesetzte Fragebogen sHAIS-Q erwies sich als praxistauglich und zuverlässig, was eine gezielte Weiterverwendung in klinischen Kontexten ermöglicht. Die Analysen zeigen, dass Wissen und Einstellungen zur Informationssicherheit bei den Mitarbeitenden insgesamt gut ausgeprägt sind. Unterschiede zeigen sich insbesondere im sicherheitsbezogenen Verhalten, das stark von arbeitsplatzbezogenen Faktoren geprägt ist. Daraus ergibt sich eine zentrale Implikation für künftige Awareness-Maßnahmen: Diese sollten nicht allein auf die Vermittlung von Wissen abzielen, sondern stärker an den konkreten Arbeitsrealitäten ansetzen. Besonders wichtig ist es, strukturelle Hürden zu identifizieren und abzubauen, praxisrelevante Schulungsformate bereitzustellen und das Personal aktiv in die Gestaltung sicherheitsrelevanter Prozesse einzubeziehen. Auch das Commitment der Führungsebene sowie der Zugang zu klaren Regeln und unterstützenden Ressourcen spielen eine entscheidende Rolle. Die Förderung von Selbstwirksamkeit, ein besseres Verständnis für die Sicherheitskultur sowie der Abbau informeller Schattenprozesse sollten integraler Bestandteil einer ganzheitlichen ISA-Strategie sein. Auf dieser Grundlage lassen sich realitätsnahe, akzeptierte und wirksame Maßnahmen zur Stärkung der Informationssicherheit in medizinischen Einrichtungen entwickeln.

# 6 Gender Mainstreaming Aspekte

Im MedISA-Projekt wurde Gendermainstreaming systematisch berücksichtigt, indem geschlechterbezogene Aspekte bereits in der Konzeption der Erhebungen und Analysen explizit mitgedacht wurden. So erfolgte in den qualitativen Interviews, Workshops und Fokusgruppen eine gezielte Auswahl von Teilnehmenden unterschiedlicher Geschlechter, um vielfältige Perspektiven auf Informationssicherheit im klinischen Alltag zu erfassen. In der quantitativen Erhebung wurde das Geschlecht der Befragten entweder systematisch in einem ausgeglichenen Verhältnis rekrutiert oder bei der Auswertung statistisch kontrolliert, um etwaige geschlechtsspezifische Unterschiede im Informationssicherheitsbewusstsein sichtbar zu machen. Darüber hinaus wurden alle Materialien und Kommunikationsformate geschlechtergerecht formuliert, um eine inklusive Ansprache sicherzustellen. Diese Maßnahmen tragen dazu bei, die Wirksamkeit von ISA-Maßnahmen geschlechterübergreifend zu erhöhen und strukturelle Benachteiligungen zu vermeiden.

# 7 Diskussion der Ergebnisse, Gesamtbeurteilung

Das MedISA-Projekt verfolgte das Ziel, praxistaugliche, evidenzbasierte und partizipativ entwickelte Maßnahmen zur Förderung der Informationssicherheits-Awareness (ISA) in medizinischen Versorgungseinrichtungen zu konzipieren, zu evaluieren und verfügbar zu machen. Im Mittelpunkt stand dabei die Frage, wie ISA-Maßnahmen möglichst wirksam und gleichzeitig ressourcenschonend in den komplexen und oft stark belasteten Klinikalltag integriert werden können. Die Projektziele wurden entlang eines strukturierten Arbeits- und Zeitplans bearbeitet und in fünf Arbeitspakete (AP1 bis AP5) operationalisiert. Die Ergebnisse zeigen, dass die gesteckten Ziele zu einem großen Teil erreicht wurden, sowohl in Bezug auf die inhaltliche Entwicklung als auch auf die methodische und praktische Umsetzbarkeit, und dass mit dem psychometrischen Messinstrument sogar weit über die ursprünglichen Zielsetzungen hinausgegangen wurde.

# 8 Soll-Ist-Vergleich: Zielerreichung nach Teilzielen

- **Z1 (Forschungsstand, Systematisierung):** Vollständig erfüllt durch einen fundierten Literaturüberblick, eine Erhebung der gesetzlichen Rahmenbedingungen (z. B. B3S, KRITIS) sowie die Erarbeitung eines strukturierten methodischen Fundaments.
- **Z2/Z3 (Analyse existierender Maßnahmen, Hürden & Anreize):** Erreicht. Trotz leichter Abweichung bei der Zahl der geplanten Interviews/Workshops sowie personeller und organisatorischer Einschränkungen konnte die Analyse in ausreichender Tiefe durchgeführt werden; PANACEA-Daten bestätigten oder ergänzten gezielt die qualitative Basis.
- **Z4/Z5/Z6 (partizipatives Design, Entwicklung von Nudges und Materialien):** Vollständig erreicht. Auf Basis von neun Workshops und Fokusgruppen sowie einer ergänzenden Literaturrecherche konnten insgesamt 56 konkrete Nudge-Ideen entwickelt und elf technisch einfach umsetzbare Nudges zur Prävention von Phishing identifiziert werden. Zudem wurde ein bestehendes psychometrisches Messinstrument überarbeitet und in einer effizienten, validierten Kurzversion (sHAIS-Q) verfügbar gemacht. Darüber hinaus wurden praxisnahe Untersuchungsdesigns entwickelt, die unter realistischen Bedingungen kausale Rückschlüsse ermöglichen. Durch den Rückgriff auf das EU-PANACEA-Toolkit konnten acht relevante Schulungsvideos identifiziert sowie der AIDE-Ansatz als strukturierende Grundlage für die partizipative Entwicklung von Nudges erfolgreich eingebunden werden.
- **Z7 (Evaluation):** Fokussiert erreicht. Die psychometrische Validierung des erweiterten HAIS-Q sowie der kompakten Kurzversion sHAIS-Q waren methodisch sehr erfolgreich. Insbesondere der Einsatz des sHAIS-Q in einer Universitätsklinik belegte die Praxistauglichkeit. Auch zwei groß angelegte Phishing-Simulationen mit über 7.000 Teilnehmenden wurden erfolgreich durchgeführt. Dabei konnten elf digitale Nudges hinsichtlich ihrer kausalen Wirksamkeit empirisch evaluiert und nach Personalgruppen differenziert ausgewertet werden. Ursprünglich geplante Langzeitevaluationen zur Nachhaltigkeit digitaler Phishing-Nudges konnten wegen organisatorischen Angelegenheiten der Klinik und aufgrund der zeitlichen Begrenzung des Projekts nicht umgesetzt werden. Die im Rahmen der Workshops entwickelten 56 Nudging-Ideen konnten ebenfalls nicht mehr konkret in der Praxis umgesetzt und getestet werden, bieten aber eine ideale Grundalge für Folgeprojekte. Hinzu kam, dass die Evaluation der PANACEA-Videos scheiterte, da einzelne Projektpartner kurzfristig absprangen oder die

Durchführung des vorgesehenen Forschungsdesigns durch die beteiligte Universitätsklinik nicht sachgerecht erfolgte.

- **Z8 (Transfer & Dissemination):** Erreicht durch Website, Maßnamenkatalog, Medienarbeit, Fachartikel und einer DMEA-Präsentation.

## Projektverlauf und Herausforderungen

Der Projektverlauf war durch mehrere unerwarteten Herausforderungen geprägt: unbesetzte Stellen, Ausfallzeiten durch Elternzeit, Streiks und einem IT-Sicherheitsvorfall in Partnerkliniken, sowie langwierige Abstimmungsprozesse mit Personalvertretungen führten zu Verzögerungen und teilweisen Plananpassungen. Durch flexible Umplanung, methodische Substitutionen (z. B. Rückgriff auf PANACEA-Materialien) und gezielte externe Unterstützung (z. B. Moderation von Workshops durch Drittanbieter) konnte die Zielerreichung trotz der Widrigkeiten gesichert werden.

## Gesamtbeurteilung und Wirkung

MedISA konnte klar zeigen, dass ISA-Maßnahmen dann besonders wirksam sind, wenn sie auf konkrete Zielgruppen zugeschnitten sind, partizipativ mit dem klinischen Personal entwickelt werden, organisationale, prozessbezogene, technische und individuelle Hürden explizit berücksichtigen und auf fundierten psychologischen und empirischen Modellen basieren.

Besonders hervorzuheben ist die Entwicklung und Validierung des **sHAIS-Q**, eines kompakten Instruments zur Erfassung von Wissen, Einstellung und Verhalten im Bereich der Informationssicherheit. Das Instrument erwies sich als wissenschaftlich robust, mit hoher Reliabilität und gesicherter Messinvarianz (Deutsch/Englisch), und ist zugleich im klinischen Alltag praktikabel einsetzbar, da die Bearbeitungszeit unter drei Minuten liegt. Zentral war zudem die partizipative Entwicklung von über 50 **Nudging-Ideen**, die auf dem AIDE-Modell und dem MINDSPACE-Rahmenwerk basieren. Die Spannbreite reicht von niederschwelligen Formaten wie Postern oder Team-Challenges bis hin zu technisch integrierten Maßnahmen wie visuellen Logout-Timern, voreingestellten Abmeldemechanismen oder QR-Codes auf Dienstausweisen.

In zwei groß angelegten **Phishing-Simulationen** mit insgesamt 7.044 Teilnehmenden konnten empirisch relevante Erkenntnisse zur konkreten Bedrohungslage im Krankenhauskontext gewonnen werden. Gleichzeitig zeigte sich, mit welchen Nudges sich Klick- und Login-Raten wirksam und kausal senken lassen. Besonders effektiv erwiesen sich visuelle HTML-Banner, die Zustellung von Mails in den SPAM-Ordner sowie die Deaktivierung von Links, die in einzelnen Fällen die Login-Raten um über 90 Prozent reduzierten ohne dabei die Handlungsfreiheit der Mitarbeitenden einzuschränken.

Diese Ergebnisse belegen die Wirkung von Nudges als minimalinvasive Sicherheitsinterventionen in realen Klinikprozessen.

## Generalisierbarkeit und Grenzen

Auch wenn die Projektergebnisse auf Untersuchungen in ausgewählten Universitätskliniken beruhen, sprechen mehrere Aspekte für eine vorsichtige Generalisierbarkeit. Zum einen wurden unterschiedliche Personalgruppen mit variierenden Rollen, Verantwortlichkeiten und Erfahrungsniveaus einbezogen, wodurch sich berufsübergreifende Muster erkennen lassen. Zum anderen basieren zentrale Maßnahmen und Instrumente wie der HAIS-Q oder das AIDE-Modell auf theoretisch etablierten und breit anerkannten Konzepten der Verhaltensforschung und Informationssicherheit. Diese Kombination aus Zielgruppenvielfalt und methodischer Fundierung erhöht die Wahrscheinlichkeit, dass zentrale Wirkprinzipien auch in anderen medizinischen und organisatorischen Kontexten relevant sind.

Gleichzeitig muss anerkannt werden, dass qualitative Ergebnisse und selektiv erhobene quantitative Daten nicht ohne Einschränkung auf andere Einrichtungen übertragbar sind. Unterschiede in Kultur, Struktur, Technik oder Führungspraxis können die Wirkung von ISA-Maßnahmen erheblich beeinflussen. Deshalb ist es unerlässlich, dass jede Anwendung der im Projekt entwickelten Maßnahmen durch eine kontextspezifische Anpassung und begleitende Evaluation flankiert wird. Nur so kann sichergestellt werden, dass die Maßnahmen nicht nur theoretisch fundiert, sondern auch praktisch wirksam und nachhaltig verankert sind.

## Empfehlungen für Praxis und Politik

MedISA liefert ein umfassendes Set an Maßnahmen, Strategien und Werkzeugen zur Förderung von ISA in der medizinischen Versorgung. Die wichtigsten Empfehlungen lauten:

- **Strukturelle Verankerung**: ISA muss durch Führungskräfte aktiv gefördert werden. Die Projektergebnisse zeigen, dass das wahrgenommene Engagement der Leitungsebene signifikant mit sicherheitskonformem Verhalten der Mitarbeitenden zusammenhängt. In der quantitativen Analyse war das sogenannte „Top-Management Commitment" besonders stark mit dem sicherheitsrelevanten Verhalten korreliert. Auch in den Interviews und Workshops wurde die mangelnde Unterstützung durch Führungspersonal wiederholt als zentrales Hindernis für die Umsetzung und Akzeptanz von ISA-Maßnahmen benannt. Internationale Standards wie die ISO/IEC 27001 fordern die Verantwortung der obersten Leitung für die Etablierung eines funktionierenden Informationssicherheitsmanagementsystems. Der „Tone from the Top" ist

damit nicht nur ein kulturprägender Faktor, sondern eine notwendige Voraussetzung für die Wirksamkeit und Glaubwürdigkeit von Awareness-Maßnahmen. Führungskräfte müssen das Thema sichtbar priorisieren, Ressourcen bereitstellen und ISA als strategische Aufgabe in der Organisation mittragen.

- **Partizipation stärken**: Mitarbeitende sollten nicht nur geschult, sondern aktiv in die Entwicklung, Anpassung und Auswahl von Maßnahmen einbezogen werden. Nur wenn ISA-Angebote mit dem Arbeitsalltag, den Routinen und dem Selbstverständnis des Personals kompatibel sind, können sie langfristig wirksam sein. Die partizipativen Workshops in MedISA haben gezeigt, dass die Einbindung der Zielgruppen sowohl die inhaltliche Passung als auch die Motivation zur Mitwirkung deutlich erhöht.
- **Evaluation sichern**: Der Einsatz objektiver Kennzahlen (KPIs) sowie psychometrisch fundierter Instrumente wie dem sHAIS-Q können nur im Rahmen fundierter Untersuchungsdesigns belastbare Aussagen über Reichweite, Wirkung und Nachhaltigkeit von ISA-Maßnahmen und deren Weiterentwicklung ermöglichen. Die Kombination von Messung und Untersuchungsdesign sollte daher systematisch entwickelt und implementiert werden.
- **Nudging nutzen**: Evaluieren ließen sich elf digitale Nudges im spezifischen Kontext von Phishing-Simulationen. Es zeigte sich, dass bestimmte Maßnahmen wie visuelle Banner, unterbrechende Hinweisseiten oder Link-Deaktivierung zu einer deutlichen Reduktion der Login-Raten führten. In den Fokusgruppen wurden insgesamt 56 Nudging-Ideen entwickelt, die gezielt unbewusste Entscheidungsprozesse bei der Auswahl von Handlungsalternativen adressieren, ohne dabei die Handlungsfreiheit der Mitarbeitenden einzuschränken. Diese Maßnahmen wurden jedoch im Rahmen des Projekts nicht im Feld getestet, sodass ihre Wirksamkeitsuntersuchung noch aussteht. Allerdings deuten die Ergebnisse aus den Phishing-Simulationen auf das Potenzial von Nudging-Strategien in medizinischen Versorgungseinrichtungen hin. Diese Ergebnisse zeigen, dass geringinvasive Nudging-Strategien nicht nur wirksam, sondern auch im Klinikalltag realisierbar und anschlussfähig sein können, insbesondere dann, wenn sie kontextspezifisch gestaltet und gemeinsam mit dem Personal entwickelt werden.
- **Standardisierung vorantreiben**: Die im Projekt gewonnenen Erkenntnisse und entwickelten Werkzeuge bieten eine fundierte Grundlage für die Weiterentwicklung von branchenspezifischen Standards, insbesondere dem Branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S). Um eine flächendeckende Umsetzung zu fördern, sollten ISA-Maßnahmen stärker in solche etablierten Rahmenwerke integriert

werden, jedoch immer unter Berücksichtigung kontextspezifischer Gegebenheiten und mit begleitender Evaluation.

# 9 Verbreitung und Öffentlichkeitsarbeit der Projektergebnisse

Ein zentrales Anliegen des MedISA-Projekts war die gezielte Verbreitung der Ergebnisse in Fachkreise, Praxisstrukturen und Öffentlichkeit sowie die Sicherstellung ihrer nachhaltigen Zugänglichkeit für relevante Akteure im Gesundheitswesen. Die Projektergebnisse wurden über vielfältige Kanäle verbreitet und in unterschiedlichen Formaten aufbereitet: von wissenschaftlichen Fachartikeln über praxisnahe Leitfäden bis hin zu Social-Media-Kommunikation.

## Fachöffentlichkeit und Wissenschaft

- **Internationale Fachkonferenz:**
  Ein zentraler Meilenstein war der Vortrag im Rahmen der DMEA 2025 (*NIS 2 und Resilienz: Zukunftsfähige Strategien für das Gesundheitswesen*, 10. April 2025), bei dem die Phishing-Studie mit über 7.000 Teilnehmenden von Dr. David Langer vorgestellt wurde. Die Session thematisierte regulatorische Anforderungen (NIS-2, KRITIS-Dachgesetz, B3S) und beleuchtete die Teilergebnisse von MedISA als Beispiel für resilienzfördernde Awareness-Strategien in der klinischen Praxis.

  **Abbildung 2**: Vorstellung der Phishing-Studie auf der DEMA 2025 von Dr. David Langer auf der Session: „NIS 2 und Resilienz: Zukunftsfähige Strategien für das Gesundheitswesen".


- **Publikationen (peer-reviewed):**
  Jan Tolsdorf, David Langer, and Luigi Lo Iacono. Phishing Susceptibility and the (In-)Effectiveness of Common Anti-Phishing Interventions in a Large University Hospital. Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS). 2025.

- David Langer, Jan, Tolsdorf, Luigi Lo Iacono: *Minimally invasive and to the point: scale-optimized, psychometrically validated instrument for assessing information security awareness.* In Bearbeitung, Einreichung im September 2025.
- Jan Tolsdorf, and Luigi Lo Iacono: *Nudge off security fatigue*. In Bearbeitung, Einreichung 2025 geplant.
- **Fachzeitschriftenbeiträge:**
  Jan Tolsdorf, Luigi Lo Iacono: *Gemeinsam gegen Hacker – aber wie?*, Ärzte-Zeitung, 2024.
  Jan Tolsdorf, Luigi Lo Iacono: *Sichere IT in Kliniken*, Krankenhaus Technik+Management, 2024.
  Jan Tolsdorf, Luigi Lo Iacono: *Sensibilisierung für IT-Sicherheit*, Tagesspiegel Background, 2024.
  Jan Tolsdorf, Luigi Lo Iacono: *Medizinisches Personal sensibilisieren: Bewusstsein für Gefährdungen der Patientenversorgung aus dem Cyberraum schaffen – Teil 1*. Krankenhaus Technik+Management, 2023 (7–8), S. 19–22.
  Jan Tolsdorf, Luigi Lo Iacono: *Faktor Mensch – Risiko und Chance: Informationssicherheitsbewusstsein in medizinischen Einrichtungen – Expertenansichten (Teil 2)*. Krankenhaus Technik+Management, 2023 (9), S. 22–25.

## Praxisorientierter Wissenstransfer

Ein zentrales Disseminationsprodukt ist der öffentlich zugängliche MedISA-Maßnahmenkatalog, der auf der Projektwebseite bereitgestellt wird und umfasst auf der einen Seite ISA-Maßnahmen und auf der anderen Seite Evaluations Werkzeuge. Er enthält:

- 56 Nudge-Ideen zur Förderung von Informationssicherheits-Awareness in medizinischen Einrichtungen
- 11 digitale Anti-Phishing-Nudges inklusive empirischer Evaluation ihrer Wirksamkeit insgesamt sowie zielgruppenspezifisch differenziert nach ärztlichem Dienst, Pflegedienst und Funktionsdienst, Verwaltung und Sonstigen.
- Zwei psychometrisch validierte Messinstrument in deutscher (und englischer) Sprache zur Erfassung von Informationssicherheitsbewusstsein: Erweiterter HAIS-Q für eine umfassende und die Kurversion sHAIS-Q für die effiziente Messung der Informationssicherheits-Awareness.
- ein Set an KPIs zur klinikbezogenen objektiven Evaluation der Awareness als auch der Wirksamkeit von Awareness-Maßnahmen

Diese Inhalte wurden in enger Abstimmung mit Fachkräften aus Medizin, Pflege, IT, Stabsstellen für Informationssicherheit und der Verwaltung verschiedener Universitätskliniken und verwandten Dienstleistungsunternehmen partizipativ entwickelt und können von weiteren medizinischen Versorgungseinrichtungen direkt übernommen oder angepasst werden.

## Öffentlichkeitsarbeit über soziale Medien

Die zentralen Ergebnisse der im Rahmen der DMEA 2025 vorgestellten Phishing-Studie wurden zusätzlich über LinkedIn in zwei Beiträgen verbreitet (eine Ankündigung sowie ein Post mit den Kernergebnissen des Vortrags) und erreichten insgesamt 1.725 Impressionen, 880 Ansichten sowie zahlreiche Reaktionen und Kontaktanfragen.

## Zugänglichkeit und Verstetigung

Die zentralen Projektergebnisse sind dauerhaft über die zweisprachige Projektwebseite abrufbar. Neben dem Maßnahmenkatalog stehen dort auch begleitende Informationen zum Projekt. Zudem können die Ergebnisse in künftige Standardisierungsvorhaben eingebracht werden, insbesondere im Rahmen des Branchenspezifischen Sicherheitsstandards (B3S) für die Gesundheitsversorgung im Krankenhaus.

# 10 Verwertung der Projektergebnisse (Nachhaltigkeit / Transferpotential)

Die im MedISA-Projekt erzielten Ergebnisse verfügen über ein hohes Transferpotenzial und leisten einen konkreten Beitrag zur Weiterentwicklung der Informationssicherheit im Gesundheitswesen. Besonders relevant für den Transfer in Praxis und Politik sind die entwickelten, evidenzbasierten Awareness-Maßnahmen sowie das psychometrisch validierte Instrument zur Messung von Informationssicherheitsbewusstsein (sHAIS-Q), das bereits im klinischen Regelbetrieb einsetzbar ist. Auch der strukturierte Maßnahmenkatalog und die erarbeiteten KPIs liefern eine direkt anwendbare Grundlage für Einrichtungen der medizinischen Versorgung, um ISA-Maßnahmen wirksam und differenziert umzusetzen sowie zu evaluieren.

## Relevanz für Gesetzgebung und Politik

Die Ergebnisse bieten eine fundierte Grundlage für gesetzgeberische Überlegungen und Normen im Kontext von NIS-2-Umsetzung, KRITIS-Dachgesetz und branchenspezifischen Sicherheitsstandards wie dem B3S. Die Projektstudien verdeutlichen, welche Faktoren die Resilienz gegenüber Cyberangriffen beeinflussen und welche Herausforderungen und Widerstände überwunden werden müssen, um ISA-Maßnahmen wirksam in hoch belasteten Versorgungseinrichtungen zu verankern. Die Erkenntnisse zu digitalem Anti-Phishing-Nudging, Phishing-Anfälligkeit und zielgruppenspezifischer Sicherheitskommunikation können dabei helfen, praxisnahe Leitlinien und realistische Mindestanforderungen zu formulieren.

## Nachhaltigkeit und Weiterentwicklung

Um die im Projekt MedISA aufgebauten Strukturen und Erkenntnisse über das Projektende hinaus nachhaltig zu sichern, ist im Rahmen des BMFTR-Förderprogramms StartUpSecure die **Gründung eines Start-ups** in Vorbereitung (die Forschenden des MedISA-Projekts sind im Juni 2025 als Gründerteam zum Einreichen eines Vollantrags aufgefordert worden). Dieses soll auf den Ergebnissen des Projekts aufbauen und verfolgt das Ziel, die kausale Wirksamkeit von ISA-Maßnahmen systematisch weiter zu erforschen. Darüber hinaus sollen praxisnahe und skalierbare Lösungen für medizinische Einrichtungen sowie Organisationen anderer sicherheitskritischer Branchen entwickelt werden. Im Zentrum stehen dabei insbesondere Evaluationsverfahren, mit denen Sicherheitsmaßnahmen kontinuierlich, zielgruppenspezifisch und evidenzbasiert bewertet und weiterentwickelt werden können.

## Weitere Implikationen und Forschungsfragen

Aus dem Projekt ergeben sich drei weiterführende Fragestellungen, die in möglichen Folgeprojekten adressiert werden können:

- Langfristige Evaluation von Anti-Phishing-Nudges und deren nachhaltiger Wirkung auf das Nutzerverhalten über längere Zeiträume hinweg
- Praxistest der 56 entwickelten Nudging-Ansätze im klinischen Alltag, um deren Umsetzbarkeit, Akzeptanz und tatsächliche Wirksamkeit unter Realbedingungen zu bewerten
- Entwicklung von low-intervention Messmethoden, die eine valide quantitative Erfassung des Nutzerverhaltens ermöglichen, ohne dabei den Arbeitsfluss des Personals zu beeinträchtigen
- Erweiterung und Verfeinerung objektiver KPIs, um verhaltensbasierte ISA analysieren zu können

# 11 Publikationsverzeichnis

- Artikel „Gemeinsam gegen Hacker – aber wie?“, Ärzte-Zeitung
- Artikel „Sichere IT in Kliniken“, Krankenhaus Technik+Management
- Artikel „Sensibilisierung für IT-Sicherheit“, Tagesspiegel Background
- Jan Tolsdorf, and Luigi Lo Iacono. Medizinisches Personal sensibilisieren: Bewusstsein für Gefährdungen der Patientenversorgung aus dem Cyberraum schaffen – Teil 1. Krankenhaus Technik+Management (KTM), 2023(7-8), p. 19-22, 2023.
- Jan Tolsdorf, and Luigi Lo Iacono. Faktor Mensch: Risiko und Chance: Informationssicherheitsbewusstsein in medizinischen Einrichtungen – Expertenansichten (Teil 2). Krankenhaus Technik+Management (KTM), 2023(9), p. 22-25, 2023.
- J. Tolsdorf and L. Lo Iacono:Expert Perspectives on Information Security Awareness Programs in Medical Care Institutions in Germany," in HCI for Cybersecurity, Privacy and Trust: 6th International Conference, HCI-CPT 2024, Held as Part of the 26th HCI International Conference, HCII 2024, Washington, DC, USA, June 29–July 4, 2024, Proceedings, Part II, Berlin, Heidelberg: Springer-Verlag, Jun. 2024, pp. 98–117. doi: 10.1007/978-3-031-61382-1_7.
- Anita Hermann: *Entwicklung, Durchführung und Auswertung eines partizipativen Workshops mit Pflegepersonal in einer medizinischen Versorgungseinrichtung zur Erarbeitung zielgruppenspezifischer ISA-Maßnahmen*, Masterarbeit im Studiengang Informatik M.sc., 2025.
- Jan Tolsdorf, David Langer, and Luigi Lo Iacono. Phishing Susceptibility and the (In-)Effectiveness of Common Anti-Phishing Interventions in a Large University Hospital. Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS). 2025.
- David Langer, Jan, Tolsdorf, Luigi Lo Iacono: *Minimally invasive and to the point: scale-optimized, psychometrically validated instrument for assessing information security awareness.* In Bearbeitung, Einreichung im September 2025.
- Jan Tolsdorf, and Luigi Lo Iacono: *Nudge off security fatigue*. In Bearbeitung, Einreichung 2025 geplant.

# 12 Literaturverzeichnis


[1] Bundesamts für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2024“, 2024, Zugegriffen: 21. Juni 2025. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5

[2] European Union Agency for Cybersecurity., *ENISA threat landscape 2023: July 2022 to June 2023.* LU: Publications Office, 2023. Zugegriffen: 21. Juni 2025. [Online]. Verfügbar unter: https://data.europa.eu/doi/10.2824/782573

[3] Universitätsklinikum Düsseldorf, „Krankenhaus derzeit nur sehr eingeschränkt erreichbar – Patientenversor-gung eingeschränkt, Pressemitteilung vom 10.09.2020“. 2020.

[4] „Wie der Hackerangriff der Frankfurter Uniklinik schadet“, *FAZ.NET*, 12. Oktober 2023. Zugegriffen: 21. Juni 2025. [Online]. Verfügbar unter: https://www.faz.net/aktuell/rhein-main/frankfurt/wie-der-hackerangriff-der-frankfurter-uniklinik-schadet-19238456.html

[5] Deutsche Krankenhaus Gesellschaft, „Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus“, Oktober 2019. Zugegriffen: 20. März 2022. [Online]. Verfügbar unter: 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

[6] E. Amankwa, M. Loock, und E. Kritzinger, „A conceptual analysis of information security education, information security training and information security awareness definitions“, in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, Dez. 2014, S. 248–252. doi: 10.1109/ICITST.2014.7038814.

[7] L. Jaeger, „Information Security Awareness: Literature Review and Integrative Framework““, in *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS*, 2018, S. 4703–4712.

[8] M. Siponen, „Siponen, M.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8(1), 31-41“, *Inf Manag Comput Secur.*, Bd. 8, S. 31–41, März 2000, doi: 10.1108/09685220010371394.

[9] Bulgurcu, „Cavusoglu und Benbasat, ‚Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness‘“, *MIS Q Bd*, Bd. 34, Nr. 3, S. 523-548, 2010, doi: 10.2307/25750690.

[10] A. Tsohou, M. Karyda, S. Kokolakis, und E. Kiountouzis, „Managing the introduction of information security awareness programmes in organisations“, *Eur. J. Inf. Syst.*, Bd. 24, S. 38–58, Okt. 2013, doi: 10.1057/ejis.2013.27.

[11] K. Khando, S. Gao, M. S. Islam, und A. Salman, „Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature

Review", *Comput. Secur.*, Bd. 106, S. 102267, Apr. 2021, doi: 10.1016/j.cose.2021.102267.
[12] L. Benedikt, „Information security awareness and behavior: a theory-based literature review"", *Manag Res Rev Bd*, Bd. 37, Nr. 12, S. 1049-1092, Jan. 2014.
[13] PANACEA, „PANACEA Research". Zugegriffen: 6. März 2023. [Online]. Verfügbar unter: https://www.panacearesearch.eu/
[14] S. Magalini, „Cyberthreats to Hospitals: Panacea, a Toolkit for People-Centric Cybersecurity"", *J Strateg Innov Sustain Bd*, Bd. 16, Nr. 3, Art. Nr. 3, Aug. 2021, doi: 10.33423/jsis.v16i3.4449.
[15] D. Branley-Bell *u. a.*, „Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff", Bd. 3, Nov. 2020, doi: 10.51381/adrs.v3i1.51.
[16] P. G. Hansen, „The Definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove?"", *Eur J Risk Regul Bd*, Bd. 7, Nr. 1, S. 155-174, 2016, doi: 10.1017/S1867299X00005468.
[17] Bundesministerium des Innern, „Verordnung zur Bestimmung Kritischer Infrastruk-turen nach dem BSI-Gesetz". S.
[18] D. Branley-Bell *u. a.*, „Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff", *Ann. Disaster Risk Sci.*, Bd. 3, Nr. 1, 2020, doi: 10.51381/adrs.v3i1.51.
[19] R. L. Plackett und J. P. Burman, „The design of optimum multifactorial experiments", *Biometrika*, Bd. 33, Nr. 4, S. 305–325, 1946, doi: 10.1093/biomet/33.4.305.
[20] L. Coventry *u. a.*, „Cyber-Risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour", in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Hrsg., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, S. 105–122. doi: 10.1007/978-3-030-50309-3_8.
[21] D. Branley-Bell, L. Coventry, und E. Sillence, „Promoting Cybersecurity Culture Change in Healthcare", in *The 14th PErvasive Technologies Related to Assistive Environments Conference*, in PETRA 2021. New York, NY, USA: Association for Computing Machinery, Juni 2021, S. 544–549. doi: 10.1145/3453892.3461622.
[22] K. Renaud und W. Goucher, „Health service employees and information security policies: an uneasy partnership?"", *Inf Manag Comput Secur Bd*, Bd. 20, Nr. 4, S. 296-311, Jan. 2012, doi: 10.1108/09685221211267666.
[23] S. Altamimi, K. Renaud, T. Storer, S. Kallel, F. Cuppens, und N., „"I do it because they do it": Social-Neutralisation in Information Security Practices of Saudi Medical Interns"", in *Risks and Security of Internet and Systems*, H. Kacem und Hrsg, Hrsg., Cham: Springer International Publishing, 2020, S. 227–243. doi: 10.1007/978-3-030-41568-6_15.
[24] A. R. Murphy, M. C. Reddy, und H. Xu, „Privacy practices in collaborative environments: a study of emergency department staff"", in *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, Baltimore Maryland USA: ACM, Feb. 2014, S. 269–282. doi: 10.1145/2531602.2531643.
[25] E. V. Eikey, A. R. Murphy, M. C. Reddy, und H. Xu, „Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's

understandings"", *Int J Med Inf Bd*, Bd. 84, Nr. 12, S. 1065-1075, 2015, doi: 10.1016/j.ijmedinf.2015.09.006.
[26] D. Liginlal, I. Sim, L. Khansa, und P. Fearn, „Human Error and Privacy Breaches in Healthcare Organizations: Causes and Management Strategies"", in *Proceedings of the Fifteenth Americas Conference on Information System (AMCIS*, 2009.
[27] M. S. Jalali und J. P. Kaiser, „Cybersecurity in Hospitals: A Systematic, Organizational Perspective"", *J Med Internet Res Bd*, Bd. 20, Nr. 5, S. 10059, Mai 2018, doi: 10.2196/10059.
[28] L. Coventry, P. Briggs, D. Jeske, und A. Moorsel, „SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment", in Design, User Experience, and Usability. Theories, Methods, and Tools for De-signing the User Experience", in *Lecture Notes in Computer Sci-ence*, A. Marcus und Hrsg, Hrsg., Cham: Springer International Publishing, 2014, S. 229–239. doi: 10.1007/978-3-319-07668-3_23.
[29] PANACEA, „PANACEA 2nd End User Workshop | Session 7: Secure Behaviour Nudging Tool". 12. Oktober 2020. Zugegriffen: 13. Dezember 2022. [Online]. Verfügbar unter: https://www.youtube.com/watch?v=x2_VBRM9fro
[30] P. Dolan, M. Hallsworth, D. Halpern, D. King, und I. Vlaev, *MINDSPACE: influencing behaviour for public policy"*. UK Institute for Government, 2010.
[31] P. Dolan, M. Hallsworth, D. Halpern, D. King, R. Metcalfe, und I. Vlaev, „Influencing behaviour: The mindspace way"", *J Econ Psychol Bd*, Bd. 33, Nr. 1, S. 264-277, 2012.
[32] J. Tan, L. Bauer, N. Christin, und L. F. Cranor, „Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements"", in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS), Virtual Event*, USA: ACM, Okt. 2020, S. 1407–1426. doi: 10.1145/3372297.3417882.
[33] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J. Cook, und E. E. Schultz, „Improving password security and memorability to protect personal and organizational information"", *Int J Hum-Comput Stud Bd*, Bd. 65, Nr. 8, S. 744-757, Aug. 2007, doi: 10.1016/j.ijhcs.2007.03.007.
[34] H. Sanchez und J. Murray, „Putting your passwords on self-destruct mode: Beating password fatigue"", in *Proceedings of the 12th Symposium On Usable Privacy and Security (SOUPS*, 2016.
[35] M. A. Sasse, M. Steves, K. Krol, und D. Chisnell, „The Great Authentication Fatigue – And How to Overcome It"", in *Lec-ture Notes in Computer Science*, P. L. P. R. Cross-Cultural Design und Hrsg, Hrsg., Cham: Springer International Publishing, 2014, S. 228–239. doi: 10.1007/978-3-319-07308-8_23.
[36] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, und T. Zwaans, „The human aspects of information security questionnaire (HAIS-Q): Two further validation studies", *Comput. Secur.*, Bd. 66, S. 40–51, Mai 2017, doi: 10.1016/j.cose.2017.01.004.
[37] T. Velki, K. Solic, und H. Ocevcic, „Development of Users' Information Security Awareness Questionnaire (UISAQ) — Ongoing work", in *2014 37th International*

*Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Mai 2014, S. 1417–1421. doi: 10.1109/MIPRO.2014.6859789.

[38] S. Egelman, M. Harbach, und E. Peer, „Behavior ever follows intention? A validation of the security behavior intentions scale (SeBIS)", in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, in CHI '16. New York, NY, USA: Association for Computing Machinery, 2016, S. 5257–5261. doi: 10.1145/2858036.2858265.

[39] G. Öğütçü, Ö. M. Testik, und O. Chouseinoglou, „Analysis of personal information security behavior and awareness", *Comput. Secur.*, Bd. 56, S. 83–93, Feb. 2016, doi: 10.1016/j.cose.2015.10.002.

[40] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, und H. Thapliyal, „A systematic literature review of cybersecurity scales assessing information security awareness", *Heliyon*, Bd. 9, Nr. 3, März 2023, doi: 10.1016/j.heliyon.2023.e14234.

[41] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, und C. Jerram, „Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Comput. Secur.*, Bd. 42, S. 165–176, Mai 2014, doi: 10.1016/j.cose.2013.12.003.

[42] E. P. Bettinghaus, „Health promotion and the knowledge-attitude-behavior continuum", *Prev. Med.*, Bd. 15, Nr. 5, S. 475–491, Sep. 1986, doi: 10.1016/0091-7435(86)90025-3.

[43] T. E. Miller, C. D. Booraem, J. V. Flowers, und A. E. Iversen, „Changes in knowledge, attitudes, and behavior as a result of a community-based AIDS prevention program", *AIDS Educ. Prev.*, Bd. 2, Nr. 1, S. 12–23, 1990.

[44] Q. Yi und N. Hohashi, „Comparison of perceptions of domestic elder abuse among healthcare workers based on the Knowledge-Attitude-Behavior (KAB) model", *PLOS ONE*, Bd. 13, Nr. 11, S. e0206640, Jan. 2018, doi: 10.1371/journal.pone.0206640.

[45] F. Bogner, „The Influence of Short-Term Outdoor Ecology Education on Long-Term Variables of Environmental Perspective", *J. Environ. Educ.*, Bd. 29, S. 17–29, Jan. 1998, doi: 10.1080/00958969809599124.

[46] A. Kollmuss und J. Agyeman, „Mind the Gap: Why do people act environmentally and what are the barriers to pro-environmental behavior?", *Environ. Educ. Res.*, Bd. 8, Nr. 3, S. 239–260, Aug. 2002, doi: 10.1080/13504620220145401.

[47] T. Kizildeniz und F. Bozkurt, „Evaluating Climate Change Knowledge, Attitudes, and Behaviors (KAB) in Agricultural Sciences and Technologies Education", *Karadeniz Fen Bilim. Derg.*, Bd. 14, S. 619–633, Mai 2024, doi: 10.31466/kfbd.1400642.

[48] S. van der Linden, „Towards a new model for communicating climate change", *Underst. Gov. Sustain. Tour. Mobil. Psychol. Behav. Approaches*, S. 243–275, März 2014.

[49] H. A. Kruger und W. D. Kearney, „A prototype for assessing information security awareness", *Comput. Secur.*, Bd. 25, Nr. 4, S. 289–296, Juni 2006, doi: 10.1016/j.cose.2006.02.008.

[50] J. Kaur und N. Mustafa, „Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME“, in *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, Nov. 2013, S. 286–290. doi: 10.1109/ICRIIS.2013.6716723.
[51] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, und C. Jerram, „A study of information security awareness in Australian government organisations“, *Inf. Manag. Comput. Secur.*, Bd. 22, Nr. 4, S. 334–345, Okt. 2014, doi: 10.1108/IMCS-10-2013-0078.
[52] L. Coventry, „Cyber-Risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour““, in *Proceedings of the 2nd International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT), A*, H. Moallem, Hrsg., Cham: Springer International Publishing, 2020, S. 105–122. doi: 10.1007/978-3-030-50309-3_8.
[53] J. Harkness, „Questionnaire Translation“, in *Cross-cultural survey methods*, J. A. Harkness, F. J. R. van de Vijver, und P. P. Mohler, Hrsg., in Wiley series in survey methodology. , Hoboken, N.J: J. Wiley, 2003, S. 35–56.
[54] B. Dorer und E. Krajčeva, „ESS Round 11 Verification Instructions for National Coordinators“.
[55] J. P. Stevens, *Applied Multivariate Statistics for the Social Sciences*, 4. Aufl. Erlbaum, 2002.
[56] H. Wu und R. Estabrook, „Identification of Confirmatory Factor Analysis Models of Different Levels of Invariance for Ordered Categorical Outcomes“, *Psychometrika*, Bd. 81, Nr. 4, S. 1014–1045, Dez. 2016, doi: 10.1007/s11336-016-9506-0.
[57] F. F. Chen, „Sensitivity of Goodness of Fit Indexes to Lack of Measurement Invariance“, *Struct. Equ. Model. Multidiscip. J.*, Bd. 14, Nr. 3, S. 464–504, Juli 2007, doi: 10.1080/10705510701301834.
[58] D. L. Putnick und M. H. Bornstein, „Measurement invariance conventions and reporting: The state of the art and future directions for psychological research“, *Dev. Rev. DR*, Bd. 41, S. 71–90, Sep. 2016, doi: 10.1016/j.dr.2016.06.004.
[59] S. Egelman und E. Peer, „Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)““, in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, in CHI '15*, New York, NY, USA: Association for Computing Machinery, Apr, 2015, S. 2873–2882. doi: 10.1145/2702123.2702249.
[60] T. Schmidt, C. Nøhr, und R. Koppel, „A simple assessment of information security awareness in hospital staff across five Danish regions“, in *Studies in health technology and informatics*, Bd. 281, 2021. doi: 10.3233/SHTI210248.