HMD Praxis der Wirtschaftsinformatik
https://doi.org/10.1365/s40702-026-01261-4

SCHWERPUNKT

Security Awareness als institutionelles Anliegen: Voraussetzungen, Herausforderungen und Gestaltungsräume für NRW-Hochschulen

Miriam Naß · Norbert Pohlmann · Stephanie Scheja · Andreas Harrer

Eingegangen: 29. September 2025 / Angenommen: 11. Februar 2026

Zusammenfassung Jüngste Ransomware-Vorfälle an deutschen Hochschulen verdeutlichen, wie die fortschreitende Digitalisierung von Forschung, Lehre und Verwaltung die Angriffsfläche erhöht und Security Awareness zur strategischen Führungsaufgabe macht. Der Beitrag positioniert Awareness im Spannungsfeld von Offenheit, Resilienz und digitaler Souveränität. Theoretisch werden verhaltens- und lernpsychologische Modelle (u. a. Self-Determination Theory und Theory of Planned Behavior) mit organisationsbezogenen Perspektiven zu Governance, Kultur und Kommunikation verknüpft. Ein besonderes Augenmerk gilt dem E-Learning als zentralem Hebel.

Auf dieser Basis wurden theoriebasierte Annahmen abgeleitet und methodisch mithilfe von leitfadengestützten Experteninterviews mit Informationssicherheitsbeauftragten und IT-Verantwortlichen mehrerer Hochschulen validiert. Die Ergebnisse verdichten aktuelle Praxiserfahrungen, wie beispielsweise das frei verfügbare Angebot *SecAware.nrw,* und identifizieren dabei drei Kernprobleme: knappe personelle und finanzielle Ressourcen, unklare Zuständigkeiten/Governance sowie eine stark heterogene Zielgruppe.

✉ Miriam Naß · Norbert Pohlmann
Institut für Internet-Sicherheit, Westfälische Hochschule Gelsenkirchen, Gelsenkirchen, Deutschland
E-Mail: nass@internet-sicherheit.de

Norbert Pohlmann
E-Mail: pohlmann@internet-sicherheit.de

Stephanie Scheja · Andreas Harrer
Institut für Digitalisierung von Lebens- und Arbeitswelten, Fachhochschule Dortmund, Dortmund, Deutschland

Stephanie Scheja
E-Mail: stephanie.scheja@fh-dortmund.de

Andreas Harrer
E-Mail: andreas.harrer@fh-dortmund.de

Published online: 24 February 2026

Der Beitrag leitet Handlungsempfehlungen für die Hochschulpraxis ab und schließt mit einer Forschungsagenda, welche die Nutzerperspektiven skizziert und motivationsbezogene psychologische Mechanismen in der Gestaltung von E-Learning-Maßnahmen stärker berücksichtigt. So können E-Learning-basierte Maßnahmen zielgruppengerecht weiterentwickelt und eine nachhaltige Sicherheitskultur im Hochschulbereich etabliert werden.

Schlüsselwörter Security Awareness · Cybersicherheit an Hochschulen · E-Learning · Informationssicherheit · Selbstlernmaterial

Security Awareness as an Institutional Concern: Requirements, Challenges, and Design Spaces for Universities in North Rhine-Westphalia

Abstract Recent ransomware incidents at higher education institutions in Germany illustrate how the ongoing digitalization of research, teaching, and administration increases vulnerability and makes security awareness a strategic management task. This article explains awareness at the intersection of openness, resilience, and digital sovereignty. Theoretically, behavioral and learning psychology models (including Self-Determination Theory and the Theory of Planned Behavior) are linked with organizational perspectives on governance, culture, and communication. Emphasis is placed on e-learning as a key element.

Based on this, theory-based assumptions were derived and methodologically validated through semi-structured expert interviews with information security officers and IT managers from several higher education institutions. The findings consolidate current practical experiences, among them the freely available offer *SecAware.nrw,* and identify three core problems: limited human and financial resources, unclear responsibilities and governance, and a highly heterogeneous target group.

The paper derives practical recommendations for higher education and concludes with a research agenda that outlines user perspectives and takes greater account of motivation-related psychological mechanisms in the design of e-learning measures. This allows e-learning-based measures to be further developed in line with the target group and a sustainable safety culture to be established in higher education.

Keywords Security Awareness · Cybersecurity in Higher Education · E-learning · Information Security · Self-learning Material

1 Einleitung

Die Digitalisierung prägt Forschung, Lehre und Verwaltung: Cloud-Systeme, E-Learning, vernetzte Labore und der Zugriff auf sensible Daten mit privaten Endgeräten kennzeichnen den „digitalen Campus“. Dadurch werden Hochschulen jedoch zunehmend zu attraktiven Zielen für cyberkriminelle Gruppen. Sicherheitsbehörden stufen die Bedrohungslage als „extrem hoch“ ein: Allein 2023 registrierte

das Bundesamt für Sicherheit in der Informationstechnik (BSI) 23 Ransomware-Angriffe auf Bildungs- und Forschungseinrichtungen; in mehreren Fällen waren explizit Universitäten betroffen (BSI 2023). Heterogene IT-Landschaften, wertvolle Datenbestände und neue Angriffsmethoden, etwa durch Künstliche Intelligenz (KI)-gestützte Phishing[1]- oder Deepfake[2]-Techniken, erhöhen das Risiko (Hochschulrektorenkonferenz 2025). Hochschulen stehen damit im Spannungsfeld zwischen Offenheit, Resilienz und digitaler Souveränität: Sie müssen Forschungsfreiheit und internationale Kooperation sichern, gleichzeitig aber ihre IT-Systeme gegen immer professionellere Angriffe schützen. Dass dies nicht immer gelingt, zeigte beispielsweise der Angriff auf die Universität Duisburg-Essen 2022/2023 mit monatelangen Betriebsausfällen.

Technische Schutzmaßnahmen allein reichen nicht aus, eine zentrale Rolle spielt der „Faktor Mensch“. Studien zeigen, dass ein erheblicher Anteil von IT-Sicherheitsvorfällen auf Fehlverhalten zurückgeht. Zeitdruck, kognitive Überlastung und fehlendes Wissen führen zu unbedachten Klicks oder riskanten Handlungen, die Angreifern Tür und Tor öffnen (Schütz 2018; Alqahtani 2022). Awareness-Programme setzen daher auf Sensibilisierung und Training, um IT-Sicherheitsverhalten zu fördern. Ein besonders flexibler Ansatz sind E-Learning-Angebote, die sich in den Studien- und Arbeitsalltag integrieren lassen und deren Wirksamkeit durch die Theorie erklärbar ist (siehe Kapitel 2). Dieses Zusammenspiel aus menschlicher Verwundbarkeit durch Fehlverhalten und nachweisbar wirksamen Interventionen verdeutlicht, warum Security-Awareness-Programme zu einem strategischen Thema der Hochschulleitung werden müssen.

Gesetzliche Vorgaben verstärken zudem den Handlungsdruck. Die europäische Network and Information Security, kurz NIS2-Richtlinie (2022) verpflichtet Mitgliedstaaten zu höheren Sicherheitsstandards, Vorfallsmanagement und Mitarbeiterschulungen. In Deutschland wurde die Richtlinie durch das NIS2-Anpassungs- und Umsetzungsakt-Gesetz umgesetzt, das am 13.11.2025 verabschiedet wurde. Nordrhein-Westfalen geht voran: Seit Beginn 2024 schreibt das Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen und Digitale Hochschule NRW (2023) mit der Vereinbarung zur Cybersicherheit (VzC) den IT-Grundschutz, Zwei-Faktor-Authentifizierung, Notfallpläne und verpflichtende Schulungen vor. Das Land finanziert dazu Personal- und Beratungskosten in Millionenhöhe. Bereits 2023 hatte die Vereinbarung zur Informationssicherheit (VzI) an Hochschulen die Einstellung von Chief Information Security Officers (CISOs) festgelegt.

Parallel entstand mit *SecAware.nrw* ein landesweites, webbasiertes Selbstlernangebot für Hochschulangehörige in Nordrhein-Westfalen. Es ist modular aufgebaut, als Website und als Open Educational Resource (OER) zum Download verfügbar, sowie darauf ausgelegt, Lerneinheiten flexibel in den Hochschulalltag zu integrieren.

[1] *Phishing* bezeichnet Täuschungsversuche, bei denen Angreifende über gefälschte E-Mails oder Websites vertrauliche Informationen erlangen (z. B. Passwort, Kreditkartennummer) oder zu schädlichen Handlungen verleiten (SecAware 2023).

[2] *Deepfakes* sind synthetische Medieninhalte die mithilfe von KI erstellt werden. Diese künstlich erzeugten oder veränderten Videos, Bilder oder Tonaufnahmen, wirken so realistisch, dass sie nur schwer als nicht originale Inhalte zu erkennen sind (SecAware 2023).

Die Inhalte liegen in mehreren Formaten vor (u. a. kurze Informations- und Lernelemente sowie interaktive Wissensüberprüfungen wie Quizfragen) und können in hochschuleigene Lernmanagementsysteme (LMS, z. B. Moodle/ILIAS) eingebunden werden. Ziel ist die Sensibilisierung für typische Angriffsmuster (z. B. Phishing und Social Engineering[3]) sowie die Stärkung anwendungsnaher Handlungsfähigkeit im Umgang mit Sicherheitsvorfällen (S*ecAware.nrw* 2025).

Der Beitrag positioniert Security Awareness als institutionelle Aufgabe. Er untersucht didaktische, organisatorische und kulturelle Voraussetzungen für nachhaltige Programme, nutzt verhaltenspsychologische und lernwissenschaftliche Modelle als Rahmen und bezieht Praxiserfahrungen von Hochschul-CISOs ein. Die Diskussion umfasst einen Abgleich zwischen theoretischen Anforderungen und praktischer Realität. Abschließend zieht der Beitrag ein Fazit über Potenziale und Risiken (sowie den zukünftigen Forschungsbedarf), um Security Awareness als festen Bestandteil der Hochschulkultur zu verankern.

2 Theorie

Security Awareness im Hochschulkontext ist eine komplexe Herausforderung. Ziel ist es nicht nur, Wissen zu vermitteln, sondern eine heterogene Zielgruppe aus Studierenden, Lehrenden und Mitarbeitenden mit unterschiedlichen Wissensständen, Erfahrungen und Motivationen wirksam zu erreichen. Nachhaltige Verhaltensänderungen lassen sich nur erzielen, wenn psychologische Mechanismen berücksichtigt werden, die menschliches Verhalten, Motivation und Lernen steuern.

Die interdisziplinäre Verbindung von Psychologie, Organisationsforschung und E-Learning eröffnet hier einen erfolgversprechenden Ansatz. Im Folgenden werden zentrale psychologische Theorien auf das E-Learning-Angebot *SecAware.nrw* bezogen und deren Relevanz für langfristige Verhaltensänderungen im Bereich Cybersicherheit herausgearbeitet.

2.1 Motivation als Schlüssel für Verhaltensänderung

Viele Awareness-Kampagnen scheitern, weil sie ausschließlich auf Wissensvermittlung setzen (Schuktomow et al. 2023; Scholl et al. 2023). Aus psychologischer Sicht ist dies unzureichend, da Wissen allein nicht zu stabilem Sicherheitsverhalten führt. Entscheidend ist die Motivation, die das Bindeglied zwischen Einstellung und Verhalten bildet. Die Intention, ein Verhalten auszuführen, entsteht durch individuelle Einstellungen, subjektive Normvorstellungen und die wahrgenommene Handlungskontrolle (Ajzen 1991).

Ein geeignetes Rahmenmodell ist die Self-Determination Theory (SDT) (Deci und Ryan 2000). Sie besagt, dass nachhaltige Motivation durch die Befriedigung der drei psychologischen Grundbedürfnisse entsteht: Autonomie, Kompetenz und

[3] *Social Engineering* ist eine Beeinflussung von Menschen, mit dem Ziel, bei ihnen bestimmte Verhaltensweisen hervorzurufen oder Handlungen zu provozieren, die sie eigentlich nicht umsetzen würden (SecAware 2023).

soziale Eingebundenheit. Im Kontext von E-Learning können diese Bedürfnisse gezielt angesprochen werden: durch die Wahlfreiheit bei Inhalten (Autonomie), durch unmittelbares Feedback und sichtbare Lernerfolge (Kompetenz) sowie durch eine Anbindung an den sozialen Raum Hochschule, etwa in Form von Austauschmöglichkeiten oder Teilnahmezertifikaten (soziale Eingebundenheit).

Studien im Hochschulkontext zeigen, dass SDT-basierte Gestaltungselemente in Online-Lernumgebungen zu höherer Lernpersistenz führen (Hartnett 2016; Jeno et al. 2019; He et al. 2025). Geary et al. (2023) betonen zudem, dass insbesondere Autonomie den Studienerfolg und die Zufriedenheit in E-Learning-Szenarien vorhersagt. Vor diesem Hintergrund erscheinen Gestaltungselemente aus dem Bereich der Serious Games[4] wie auch systematisch eingesetzte Gamificationelemente[5] als äußerst passende Instrumente zur Steigerung von Motivation, Lernengagement und Persistenz (Hamari et al. 2014, 2016). Solche Elemente finden sich beispielweise in Form von interaktiven Elementen als Teil des *SecAware.nrw*-Lernangebots. So können die Themen spielerisch erfahren und verinnerlicht werden.

Ein möglicher Zielkonflikt zwischen dem SDT-Bedürfnis nach Autonomie und der in der Praxis teilweise umgesetzten Verbindlichkeit – etwa verpflichtenden Awareness-Schulungen für Mitarbeitende im Rahmen der VzC – lässt sich durch eine Differenzierung adressieren: Verbindlichkeit kann sich auf Teilnahme und Nachweis beziehen (Governance/Compliance), während Autonomie im Lernprozess erhalten bleibt (didaktisches Design). SDT-konforme Pflichtformate ermöglichen z. B. Selbststeuerung (Zeitpunkt, Reihenfolge, Wahl von Vertiefungsmodulen), adaptive Lernpfade (Einstufung nach Vorwissen), sowie Kompetenzerleben (unmittelbares Feedback, sichtbare Lernfortschritte) und soziale Eingebundenheit (hochschulbezogene Fallbeispiele, Anerkennung durch Zertifikate). Dadurch können auch verpflichtende Angebote motivationspsychologisch anschlussfähig gestaltet werden (Armas und Taherdoost 2025).

2.2 Von Wissen zu Verhalten: Psychologische Mechanismen der Awareness

Modelle aus der Verhaltenspsychologie wie die Theory of Planned Behavior (Ajzen 1991) oder die Taxonomie intentionalen und unintentionalen Cybersecurity-Verhaltens von Mashiane und Kritzinger (2019) verdeutlichen, dass Sicherheitsverhalten nicht allein durch Wissen entsteht. Vielmehr resultiert es aus der Wechselwirkung von Einstellungen, sozialem Druck und wahrgenommener Handlungskontrolle (Rogers 1975; Ajzen 1991; Chamroonsawasdi et al. 2017). Awareness-Maßnahmen müssen daher über reine Informationsvermittlung hinausgehen und sowohl die Handlungskompetenz als auch die Motivation der Teilnehmenden stärken.

So werden Schutzmaßnahmen dann ergriffen, wenn Menschen sich einer (gesundheitlichen) Bedrohung bewusst sind und glauben mit bestimmten Verhaltensweisen diese Bedrohung verringern zu können (Zwilling et al. 2022; Kiran et al. 2025). Effektive Programme kombinieren deshalb Wissensvermittlung mit der Möglichkeit,

[4] *Serious Games:* Spiele mit ernsthaftem Hintergrund oder Thema.

[5] *Gamificationelemente*: Nutzung von Spielelementen (z. B. Punkte sammeln oder Storytelling) außerhalb von Spielen.

Verhaltensweisen praktisch zu üben. Gerade im Bereich der Cybersicherheit ist dies zentral, da nicht nur bewusstes, sondern auch unbewusstes Handeln sicherheitskritisch sein kann (Mashiane und Kritzinger 2019). Ein reines Auswendiglernen von Regeln reicht hier nicht aus; stattdessen müssen Lernende befähigt werden, Situationen zu erkennen und intuitiv angemessen zu reagieren.

Eine zusätzliche Herausforderung besteht in der sogenannten „Security Fatigue". Ständige Sicherheitswarnungen können zu Überforderung und Resignation führen (Stanton et al. 2016). Awareness-Programme sollten daher abwechslungsreich, motivierend und alltagsnah gestaltet sein, um langfristige Wirkung zu entfalten (Bada et al. 2019).

Luo et al. (2025) zeigen, dass Autonomie, Kompetenz und Eingebundenheit eng mit intrinsischer Motivation im Online-Lernen verknüpft sind. Extrinsische Faktoren wie Leistungsdruck wirken hingegen schwächer. Auch die Analysen von Wang et al. (2024) und Shank et al. (2024) bestätigen, dass SDT-Interventionen insbesondere Selbstwirksamkeit, Autonomie und Kompetenz wirksam stärken.

2.3 Vertiefende theoretische Perspektiven

Schließlich ist auch eine organisationale Perspektive zentral. Individuelles Lernen und Motivation können ihre Wirkung nur dann dauerhaft entfalten, wenn sie institutionell eingebettet sind. Studien zeigen, dass Top-Management-Support und das Commitment der Hochschulleitung entscheidend sind, um Sicherheitsmaßnahmen nachhaltig zu verankern (McFadzean et al. 2011; Alkalbani et al. 2016). Zusätzlich schafft eine klar definierte IT-Sicherheitskultur, getragen von Führung und struktureller Verankerung wie zum Beispiel durch CISOs, Rahmenbedingungen, in denen Awareness-Prozesse nicht punktuell, sondern kontinuierlich erfolgen können (Haney und Lutters 2019, 2023; Uchendu et al. 2021). Ohne diese Unterstützung drohen Awareness-Maßnahmen isoliert zu bleiben und lediglich formaler Pflicht zu genügen. Eine solche Verzahnung von Lernprozessen und organisatorischer Integration stellt daher die Voraussetzung für die nachhaltige Etablierung von IT-Sicherheitsverhalten an Hochschulen dar und bildet zugleich die Grundlage für die im folgenden Kapitel dargestellten praktischen Herausforderungen.

3 Herausforderungen in der Hochschulpraxis

Die erfolgreiche Umsetzung von Security-Awareness-Angeboten an Hochschulen steht im Spannungsfeld technischer, organisatorischer und didaktischer Rahmenbedingungen. Während technische Schutzmaßnahmen wie Firewalls längst etabliert sind, weist die Forschung zunehmend darauf hin, dass der „Human Factor" ein zentraler Risikofaktor in der Informationssicherheit ist und maßgeblich zur Prävention von IT-Sicherheitsvorfällen beiträgt (Parsons et al. 2014; Bada et al. 2019; Maier und Aengenheyster 2020). Dennoch befassen sich nur wenige wissenschaftliche Arbeiten explizit mit diesem Faktor (Schütz 2018).

Hochschulen sind hierbei in besonderer Weise gefordert. Aus der Literatur und theoretischen Modellen lassen sich drei besonders zentrale Problemfelder ableiten.

Diese wirken oft wechselseitig verstärkend und bilden den strukturellen Rahmen, in dem Awareness-Programme geplant und umgesetzt werden. Daher werden sie nachfolgend vertieft.

3.1 Ressourcenmangel als strukturelles Hindernis

Wirksame Security-Awareness-Programme erfordern kontinuierliche Investitionen in Personal, Inhalte, technische Infrastruktur und strategische Kommunikation. Didaktisch hochwertige Formate, wie interaktive Lernelemente oder Gamification, gelten in der Forschung als besonders effektiv, sind jedoch zeit- und kostenintensiv in Entwicklung und Pflege (Tschakert und Ngamsuriyaroj 2019; Gwenhure und Sapty Rahayu 2024).

Parallel müssen Hochschulen ihre technische Grundsicherung gewährleisten, etwa durch Schwachstellenmanagement, Multi-Faktor-Authentifizierung[6] oder Notfallpläne. Awareness-Angebote konkurrieren somit mit anderen sicherheitsrelevanten Investitionen, die in Zeiten knapper Budgets ebenso erfüllt werden müssen (Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen und Digitale Hochschule NRW 2023; Wiarda 2025).

Die Personalproblematik verschärft dies, denn qualifiziertes IT-Sicherheitspersonal ist auf dem Arbeitsmarkt stark nachgefragt, wodurch Hochschulen in direkter Konkurrenz zur Privatwirtschaft stehen (European Union Agency for Cybersecurity 2024; Ministerium für Kultur und Wissenschaften des Landes Nordrhein-Westfalen 2024). Awareness-Aufgaben werden daher nicht selten zusätzlich zu den Kernaufgaben des IT-Betriebs übernommen, was deren Umfang und Qualität begrenzen kann. Die folgenden Annahmen werden in Kapitel 4 anhand der Experteninterviews praxisbezogen reflektiert:

1. Ressourcenabhängigkeit: Begrenzte finanzielle und personelle Ressourcen reduzieren Umfang, Aktualität und Interaktivität von Awareness-Angeboten.
2. Modularität und Hochschulbezug: Modular aufgebaute Angebote mit direktem Bezug zum Hochschulalltag wie *SecAware.nrw* und Anpassungsoptionen an hochschulspezifische Vorgaben werden positiver bewertet als generische Standardkurse.

3.2 Unklare Zuständigkeiten und fehlende Verbindlichkeit

Organisationssoziologische Ansätze zeigen, dass klar definierte Rollen und Verantwortlichkeiten zentrale Voraussetzungen für die erfolgreiche Implementierung neuer Maßnahmen sind (Argyris und Schön 1999; Schein 2017). Die Hochschulrektorenkonferenz (HRK) warnt, dass Hochschulen ohne klar geregelte Verantwortlichkeiten zwischen Anforderungen an Offenheit, Resilienz und digitale Souveränität aufge-

[6] *Multi-Faktor-Authentifizierung* bzw. die häufigste Variante, die *Zwei-Faktor-Authentifizierung (2FA),* bezeichnet ein Sicherheitsverfahren, bei dem neben dem Passwort ein oder mehrere weitere, einzigartige Merkmale und Faktoren genutzt werden, um die Identität zu bestätigen und sich in IT-Systemen und IT-Dienste einzuloggen (SecAware 2023).

rieben werden könnten. Internationale Standards wie ISO/IEC 27001:2022 oder das NIST Cybersecurity Framework empfehlen daher die Einrichtung einer eigenständigen, strategisch verankerten Rolle – etwa eines CISOs – mit direkter Berichtslinie an leitungsbefugte Personen. Auch das Land NRW definiert im Rahmen des Programms „Netzwerk Informationssicherheit.nrw“ Aufgabenprofile und Kompetenzen dieser Funktion.

Fehlen jedoch verbindliche Governance-Strukturen, besteht die Gefahr, dass Awareness-Maßnahmen punktuell, unsystematisch und abhängig vom Engagement Einzelner sind (Disterer 2013). Verbindlichkeit entsteht in der Regel erst, wenn Awareness-Themen institutionell verankert werden, beispielsweise durch verpflichtende Onboarding-Schulungen, die Integration in Curricula oder durch Leistungsvereinbarungen (Parsons et al. 2014; Tsohou et al. 2015). Zusammenfassend ergeben sich daraus die beiden Annahmen:

3. Governance-Einfluss: Definierte Rollen, Entscheidungskompetenzen und funktionierende Schnittstellen sind Voraussetzung für die langlebige und verbindliche Integration von Awareness-Themen in Curricula, Onboarding und Verwaltungsprozesse (im Sinne von Life-Long-Learning).
4. Institutionelle Unterstützung: Strategische Kommunikation durch die Hochschulleitung sowie verpflichtende Teilnahmevorgaben erhöhen Reichweite und Teilnahmequoten.

3.3 Heterogene Zielgruppen und didaktische Komplexität

Hochschulen vereinen Zielgruppen mit stark unterschiedlichen Rollen, Wissensständen, Motivationen und Sicherheitsbedürfnissen. Das IT-Fachpersonal hat typischerweise andere Bedarfe als etwa Bachelor-Studierende in den Geisteswissenschaften (Alshaikh 2020). Sprachliche und kulturelle Unterschiede, etwa bei internationalen Studierenden oder Mitarbeitenden, erschweren zusätzlich die Vermittlung. Die Literatur empfiehlt deshalb differenzierte Inhalte, adaptive Lernpfade und kontextbezogene Beispiele (Parsons et al. 2014; Haney und Lutters 2019).

Lernpsychologische Modelle wie die SDT verdeutlichen zudem, dass nachhaltige Verhaltensänderungen nur dann erzielt werden, wenn die Bedürfnisse nach Autonomie, Kompetenz und sozialer Eingebundenheit berücksichtigt werden (Deci und Ryan 2000). Awareness-Programme, die diese Faktoren vernachlässigen, werden schnell als bloße Pflichtübungen wahrgenommen und entfalten weniger Wirkung (Wang et al. 2024; Shank et al. 2024). Aufgrund dessen lautet die letzte Annahme:

5. Zielgruppenpassung: Unterschiedliche Rollen, Wissensstände und Motivationen erfordern differenzierte, zielgruppenspezifische Inhalte und Ansprache.

Die Experteninterviews prüfen, inwieweit diese Anpassung erfolgt und welche Zielgruppen bisher schwer erreichbar sind.

Die fünf Annahmen der drei zentralen Problemfelder bilden den Rahmen für die anschließende empirische Untersuchung und ermöglichen den systematischen Abgleich von Theorie und Praxis in den folgenden Kapiteln.

4 Punktuelle empirische Einblicke – Perspektiven von IT-Verantwortlichen auf Awareness-Angebote

Im Rahmen einer laufenden Dissertation wurden sechs leitfadengestützte Experteninterviews mit CISOs und IT-Verantwortlichen geführt, davon vier an NRW-Hochschulen und Universitäten unterschiedlicher Größe sowie zwei in hochschulübergreifenden Funktionen auf Landesebene. Ziel war eine explorative Erhebung von Governance-, Umsetzungs- und Gestaltungsperspektiven auf Security-Awareness-Maßnahmen sowie eine Validierung der in Kapitel 3 abgeleiteten theoriebasierten Annahmen. Die Interviewpartner und -partnerinnen (zwei männlich, vier weiblich) wurden gezielt über einschlägige berufliche Kontexte und Funktionsrollen angesprochen; alle Befragten kannten das landesweite Angebot *SecAware.nrw* und berichteten aus der Anwendungspraxis. Die Interviews dauerten jeweils ca. 60 min.

Die Interviews wurden entlang eines Leitfadens durchgeführt, der zentrale Dimensionen (bestehende Angebote, Motivationsfaktoren, Umsetzungsbarrieren, institutionelle Einbettung, kommunikative Sichtweisen, Zielgruppenadressierung) abdeckte. Die Auswertung erfolgte mittels qualitativer Inhaltsanalyse nach Kuckartz, einem etablierten regelgeleiteten Verfahren zur thematischen Strukturierung und Kodierung qualitativer Daten. Die Ergebnisse sind als punktuelle empirische Einblicke zu verstehen; sie erlauben eine theoriegeleitete Reflexion der Praxis, ersetzen jedoch keine repräsentative Wirkungsevaluation (Kuckartz 2018).

4.1 Bewertung vorhandener Angebote – Beispiel *SecAware.nrw*

Die Befragten setzen an ihren Hochschulen eine Kombination aus digitalen Plattformen (z. B. *SecAware.nrw*), Präsenzschulungen, Workshops, Flyer und hochschuleigenen Webseiten mit Sicherheitshinweisen ein. Positiv hervorgehoben wurden bei *SecAware.nrw* der flexible, modulare Aufbau, die Möglichkeit der Integration von OER-Lernmodulen in Lernmanagementsysteme wie Moodle oder ILIAS sowie die kontinuierliche Aktualisierung der Inhalte, um auf neue Risiken – wie etwa KI-gestützte Deepfakes – zu reagieren.

Der fallbasierte Lernansatz mit Hochschulbezug wurde als sehr motivierend bewertet, da sich die Inhalte realistisch auf den Hochschulalltag übertragen lassen. Im Vergleich dazu wirken die Formulierungen kommerzieller Anbieter oft an der Privatwirtschaft orientiert (z. B. „Geschäftsführer“ oder „Betriebsrat“), was im Hochschulkontext als wenig passend wahrgenommen wird.

Kritisch angemerkt wurde hingegen, dass die Inhalte bislang nur begrenzt auf die Bedarfe einzelner Zielgruppen zugeschnitten werden können. Gewünscht werden adaptierbare Module, die beispielsweise spezifische Ansprechpersonen oder hochschulinterne Prozesse bei Sicherheitsvorfällen berücksichtigen.

4.2 Wirksamkeitsfaktoren aus Sicht der Praxis

Die Interviews bestätigen, dass interaktive und spielerische Formate, wie Quizze, Gamification oder simulierte Phishing-Angriffe, besonders einprägsam sind. Ebenso wird betont, dass Inhalte visuell, sprachlich und kommunikativ ansprechend gestal-

tet sowie über verschiedene Kanäle verbreitet werden sollten, um vor allem bei freiwilligen Zielgruppen Aufmerksamkeit zu erzeugen.

Viele CISOs sehen hier jedoch Grenzen: Es fehlt an Kommunikations- und Marketingexpertise, um Angebote gezielt zu bewerben. Ressourcen für umfangreiche Kampagnen in Kooperation mit Hochschulkommunikation oder Social-Media-Teams stehen in der Regel nicht zur Verfügung (s. Kapitel 4.3). Aus Sicht der Befragten könnte professionelles Marketing – insbesondere für die schwer erreichbare Zielgruppe der Studierenden – Sichtbarkeit, Reichweite und Attraktivität deutlich steigern.

Darüber hinaus wünschen sich viele die aktive Unterstützung durch Hochschulleitungen. Top-down-Kommunikation, etwa durch Informationsmails des Rektorats oder die Einführung verpflichtender Schulungen, würde Awareness-Maßnahmen mehr Gewicht verleihen. Einige CISOs berichteten allerdings, dass sie die Sichtbarkeit des Themas erst durch eigenes Agenda Setting erkämpfen müssen, da Informationssicherheit institutionell noch nicht flächendeckend verankert ist.

Fehlende verbindliche Strukturen und Kommunikationswege auf Fakultäts- und Fachbereichsebene erschweren zudem die Umsetzung: Ohne Integration in Curricula und Verwaltungsprozesse bleiben strategische Vorgaben oft folgenlos. Hinzu kommt, dass CISOs in der komplexen, dezentralen Hochschullandschaft meist keine weitreichenden Entscheidungsbefugnisse besitzen.

4.3 Herausforderungen in der Umsetzung

Die in Kapitel 3 beschriebenen strukturellen Probleme spiegeln sich in den Interviews wider:

Viele CISOs verantworten gleichzeitig das Business Continuity Management (BCM) im Bereich Informationssicherheit, Incident Response, Awareness sowie weitere IT-Sicherheitsaufgaben. Übergeordnete Hochschulinstanzen berichten von Schwierigkeiten, qualifiziertes Fachpersonal zu gewinnen. Insbesondere kleinere Hochschulen für angewandte Wissenschaften schildern „One-Man-Show"-Situationen, in denen kaum Ressourcen für die kontinuierliche Pflege oder die Entwicklung eines vielfältigen Repertoires an Awareness-Maßnahmen mit zielgruppenspezifischen Anpassungen von Inhalten vorhanden sind. Infolge dieser Engpässe greifen Hochschulen teils auf externe Anbieter zurück – eine kostenintensive Lösung, die angesichts knapper Budgets kaum nachhaltig finanzierbar ist. Daher erfahren landesweit geförderte, kostenfreie Angebote wie *SecAware.nrw* hohe Zustimmung und werden positiv wahrgenommen.

Die Heterogenität der Zielgruppen bleibt eine zentrale Herausforderung. Die Befragten berichten von unterschiedlichen Anforderungen:

- Studierende benötigen oft grundlegende Informationen (z. B. Passwortsicherheit, Phishing),
- Forschende vertiefte Hinweise zum Schutz sensibler Daten,
- Verwaltungspersonal Kenntnisse zu Datenschutz- und Compliance-Vorgaben, und
- Lehrende die Fähigkeit, Sicherheitsaspekte in digitale Lehrformate zu integrieren.

Besonders Studierende, die zahlenmäßig größte, aber schwer zu erreichende Gruppe, nehmen Awareness-Angebote nur eingeschränkt wahr, solange diese frei-

willig sind. Verwaltungspersonal sind hingegen aufgrund der VzC zu jährlichen Schulungen verpflichtet. Professoren gelten ebenfalls als schwer erreichbare Zielgruppe, da für sie in der Regel keine Pflichtschulungen vorgesehen sind. Obwohl *SecAware.nrw* den Hochschulkontext aufgreift, stößt das Projekt an Grenzen, mit der Folge, dass die Inhalte in der Praxis teils zu generisch bleiben, um alle gleichermaßen ansprechen zu können.

4.4 Gestaltungsspielräume und Perspektiven

Die Befragten sehen einige Verbesserungspotenziale. Unter anderem genannt wurden:

- Stärkere Integration von *SecAware.nrw* in hochschuleigene Systeme (z. B. Zertifikate im Rahmen des Onboardings oder bei mobilem Arbeiten)
- Unterstützung durch relevante Stakeholder (z. B. Hochschulleitungen) und verpflichtende Schulungen für alle Hochschulangehörigen, nicht nur für besonders sicherheitsrelevante Bereiche
- Personalisierte Inhalte mit adaptiven Lernpfaden je nach Wissenslevel
- Spezielle Module für bestimmte Rollen (Studierende, Lehrende, Forschende, Verwaltungspersonal, IT)
- Zielgruppengerechte Ansprache oder die Etablierung neuer, niedrigschwelliger Formate wie „Informationshäppchen“ oder thematische Escape Rooms, um Aufmerksamkeit bei den Freiwilligen zu generieren

Konsens besteht darin, dass Security Awareness kein einmaliges Projekt, sondern ein kontinuierlicher Prozess ist, der institutionell und langfristig in Personalentwicklung, Curricula und Leistungsvereinbarungen integriert werden sollte. Die CISOs betonen in diesem Kontext die Relevanz der Balance zwischen Kontinuität und Überdruss, da ansonsten „Cybersicherheitsmüdigkeit“ eintreten könnte.

5 Diskussion

Die empirischen Ergebnisse bestätigen die zentralen Annahmen aus Kapitel 3, zeigen jedoch noch Weiterentwicklungsbedarfe der Angebote auf. Wie in der Theorie prognostiziert, begrenzen knappe finanzielle und personelle Ressourcen die Reichweite und Qualität von Awareness-Maßnahmen. Vor allem kleinere Hochschulen stehen vor dem Problem, dass CISOs mehrere Aufgaben parallel übernehmen müssen. In der Praxis führt dies häufig zur Nutzung standardisierter Angebote, die den Hochschulkontext nicht adressieren. Gleichzeitig ist *SecAware.nrw* eine kostenlose und aktuelle Lösung, bei der Bedarfe spezifisch für einzelne Hochschulen bisher noch nicht realisiert wurden.

Auch der theoretisch betonte Einfluss klarer Zuständigkeiten zeigt sich in den Interviews. Fehlende Governance-Strukturen und geringe Entscheidungskompetenz von CISOs erschweren die verbindliche Integration von Awareness-Themen in Curricula oder Onboarding-Prozesse. Theorie und Praxis stimmen zudem darin überein,

dass die Hochschulleitung als strategischer Unterstützer entscheidend ist. In der Umsetzung bleibt diese Einbindung jedoch oft punktuell.

Die Heterogenität der Zielgruppen erweist sich als ebenso große Herausforderung wie theoretisch beschrieben. Studierende, Lehrende, Forschende, Verwaltungspersonal und ITler benötigen stark differenzierte Inhalte, was in *SecAware.nrw* durch eine kontinuierliche Feedbackmöglichkeit adressiert wird. Besonders Studierende und Professoren gelten als schwer zu erreichende Zielgruppe. Hier könnte die in der Theorie empfohlene Modularität den Praxisbezug erhöhen oder strategische Kommunikationsmaßnahmen für Aufmerksamkeit sorgen, wird aktuell jedoch noch nicht umfassend umgesetzt.

Psychologische Faktoren wie Autonomie, Kompetenz und soziale Eingebundenheit, die in der Literatur als Treiber nachhaltiger Verhaltensänderung gelten, finden in der Praxis durch Gamification-Ansätze nur teilweise Berücksichtigung. Zudem können Medienberichte über Sicherheitsvorfälle als externer Anlass wirksam sein, um Aufmerksamkeit für Awareness-Maßnahmen zu erzeugen. Weitere Motivationsfaktoren wie persönliche Betroffenheit oder intrinsisches Eigeninteresse wurden in dieser Untersuchung nicht beleuchtet, da sie von außen nur bedingt steuerbar und schlecht skalierbar sind.

Ein weiterer Aspekt, den die Praxis hervorhebt, ist die Notwendigkeit von Geduld und Langfristigkeit, da kurzfristige Kampagnen selten nachhaltig wirken. Gerade bei dauerhaft beschäftigten Zielgruppen wie Verwaltungspersonal lohnt sich der kontinuierliche Invest. Gleichzeitig gilt es darauf zu achten, dass kein abnehmendes Interesse im Laufe der Zeit entsteht, indem Inhalte regelmäßig aktualisiert und abwechslungsreich gestaltet werden.

6 Ausblick, Handlungsempfehlungen und weiterer Forschungsbedarf

SecAware.nrw als Kompetenzzentrum hilft durch sein frei verfügbares Angebot dabei, Ressourcen effizient einzusetzen und durch Vernetzung der Stakeholder die Umsetzung von Awareness-Schulungen für heterogene Zielgruppen zu unterstützen. Auf dieser Basis lassen sich folgende Handlungsempfehlungen für die Hochschulpraxis ableiten:

- *Institutionelle Verankerung stärken:* Awareness verbindlich in Onboarding, jährliche Wiederholungen (insb. Verwaltung/risikorelevante Rollen) und, wo fachlich sinnvoll, in Curricula oder Leistungsvereinbarungen integrieren. Dazu sind klare Zuständigkeiten sowie definierte Schnittstellen zwischen CISO-Funktion, Personalentwicklung, IT-Betrieb und Hochschulkommunikation zu etablieren.
- *Verbindlichkeit SDT-konform gestalten:* Verpflichtende Formate sollten Autonomie im Lernprozess sicherstellen (Selbststeuerung, Wahlmodule, adaptive Pfade) und Kompetenz/soziale Zugehörigkeit stärken (Feedback, hochschulnahe Fälle, sichtbare Anerkennung).
- *Zielgruppenpassung ausbauen:* Inhalte entlang von Rollen, Szenarien und Systemkontexten segmentieren (Studierende, Lehrende, Forschende, Verwaltungspersonal, ITler), beispielsweise ein Modell aus Pflicht-Basismodulen plus rollenbe-

zogene Vertiefungen sowie klaren Empfehlungen je Zielgruppe (z. B. „Pflicht innerhalb von 4 Wochen nach Start“).
- *Kommunikation und Marketing professionalisieren:* Awareness als Kampagne mit konsistenten Botschaften und Kanälen planen (z. B. Teilnahme an Erstsemester-Begrüßungsveranstaltungen). Hochschulkommunikation und Studierendenservice sollten als Multiplikatoren eingebunden werden; Materialien (Kurztexte, Slides) zentral bereitstellen.
- *Integration in Prozesse und Systeme erhöhen:* E-Learning-Angebote in LMS/HR-Systeme einbinden (Single-Sign-On, automatische Nachweise), Zertifikate/Teilnahmebestätigungen als Dokumentation und Motivation nutzen.
- *Kontinuität und Aktualität sichern:* Inhalte regelmäßig aktualisieren (Bedrohungslandschaft, neue Angriffsmuster) und die „Security Fatigue“ durch Abwechslung, kurze Formate und konkrete Handlungsroutinen adressieren (z. B. „Awareness-Häppchen“).
- *Wir-Gefühl und Sicherheitskultur fördern:* Sicherheitsverhalten als Beitrag zur gemeinsamen Resilienz kommunizieren; Führungskräfte sollten sichtbares Commitment zeigen (Top-down-Signale, Vorbildverhalten, Ressourcenfreigabe).

Folgende Forschungslücken ergeben sich aus der Betrachtung der in diesem Artikel diskutierten Thematiken: Für eine abschließende Bewertung von Awareness-Maßnahmen wie *SecAware.nrw* und ähnlichen Plattformen sollte die Perspektive der Nutzenden systematisch einbezogen werden. Zukünftige Studien könnten sich mit der Wahrnehmung der Inhalte und Formate, dem Faktor Kommunikation oder konkreten didaktischen Ansätzen befassen. Langfristig erscheint es lohnend, den Einfluss psychologischer Faktoren wie intrinsische Motivation oder persönliche Betroffenheit spezifisch im Kontext von Cybersecurity zu erforschen und gezielt in die Gestaltung von Awareness-Maßnahmen zu integrieren.

Funding Open Access funding enabled and organized by Projekt DEAL.

Interessenkonflikt M. Naß, N. Pohlmann, S. Scheja und A. Harrer geben an, dass kein Interessenkonflikt besteht.

Literatur

Ajzen I (1991) The theory of planned behavior. Organ Behav Hum Decis Process 50:179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alkalbani A, Deng H, Kam B (2016) Investigating the role of socio-organizational factors in the information security compliance in organizations.
Alqahtani MA (2022) Cybersecurity awareness based on software and E-mail security with statistical analysis. Comput Intell Neurosci 2022:6775980. https://doi.org/10.1155/2022/6775980
Alshaikh M (2020) Developing cybersecurity culture to influence employee behavior: a practice perspective. Comput Secur 98:102003. https://doi.org/10.1016/j.cose.2020.102003
Argyris C, Schön DA (1999) Organizational learning II: theory, method, and practice. Addison-Wesley, Reading
Armas R, Taherdoost H (2025) Building a cybersecurity culture in higher education: proposing a cybersecurity awareness paradigm. Information 16:336. https://doi.org/10.3390/info16050336
Bada M, Sasse AM, Nurse JRC (2019) Cyber security awareness campaigns: why do they fail to change behaviour? https://doi.org/10.48550/ARXIV.1901.02672
Bundesamt für Sicherheit in der Informationstechnik (BSI) (2023) Die Lage der IT-S icherheit in Deutschland 2023
Chamroonsawasdi K, Chottanapund S, Tunyasitthisundhorn P et al (2017) Development and validation of a questionnaire to assess knowledge, threat and coping appraisal, and intention to practice healthy behaviors related to non-communicable diseases in the Thai population. Behav Sci 7:20. https://doi.org/10.3390/bs7020020
Deci EL, Ryan RM (2000) The "what" and "why" of goal pursuits: human needs and the self-determination of behavior. Psychol Inq 11:227–268. https://doi.org/10.1207/S15327965PLI1104_01
Disterer G (2013) ISO/IEC 27000, 27001 and 27002 for information security management. JIS 04:92–100. https://doi.org/10.4236/jis.2013.42011
European Union Agency for Cybersecurity (2024) ECSM 2023 campaign report: be smarter than a hacker : April 2024. Publications Office
Geary E, Allen K-A, Gamble N, Pahlevansharif S (2023) Online learning during the COVID-19 pandemic: does social connectedness and learning community predict self-determined needs and course satisfaction? J Univ Teach Learn Pract
Gwenhure AK, Sapty Rahayu F (2024) Gamification of cybersecurity awareness for non-IT professionals: a systematic literature review. IJSG 11:83–99. https://doi.org/10.17083/ijsg.v11i1.719
Hamari J, Koivisto J, Sarsa H (2014) Does gamification work?—A literature review of empirical studies on gamification. In: 2014 47th Hawaii International Conference on System Sciences. IEEE, Waikoloa, S 3025–3034
Hamari J, Shernoff D, Coller B et al (2016) Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. Comput Human Behav. https://doi.org/10.1016/j.chb.2015.07.045
Haney JM, Lutters W (2023) From compliance to impact: tracing the transformation of an organizational security awareness program
Haney JM, Lutters WG (2019) "It's scary...it's confusing...it's dull": how cybersecurity advocates overcome negative perceptions of security
Hartnett M (2016) The importance of motivation in Online learning. In: Motivation in online education. Springer Singapore, Singapore, S 5–32
He J, Wang Q, Lee H (2025) Enhancing online learning engagement: teacher support, psychological needs satisfaction and interaction. BMC Psychol 13:696. https://doi.org/10.1186/s40359-025-03016-0
Hochschulrektorenkonferenz (2025) Handlungsdruck für Hochschulen, Länder und Bund – HRK-Empfehlungen zur Cybersicherheit. https://www.hrk.de/positionen/beschluss/detail/handlungsdruck-fuer-hochschulen-laender-und-bund-hrk-empfehlungen-zur-cybersicherheit/. Zugegriffen: 18. Aug. 2025
Jeno LM, Adachi PJC, Grytnes J et al (2019) The effects of m-learning on motivation, achievement and well-being: a self-determination theory approach. Br J Educational Tech 50:669–683. https://doi.org/10.1111/bjet.12657
Kiran U, Khan NF, Murtaza H et al (2025) Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. Comput Secur 149:104204. https://doi.org/10.1016/j.cose.2024.104204
Kuckartz U (2018) Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, 4. Aufl. Beltz, Weinheim
Luo C, Hasan NAM, Zamri Bin Ahmad AM, Lei G (2025) Influence of short video content on consumers purchase intentions on social media platforms with trust as a mediator. Sci Rep 15:16605. https://doi.org/10.1038/s41598-025-94994-z
Maier S, Aengenheyster S (2020) Cyber-Security und Resilienz verstehen. In: Geschäftsrisiko Cyber-Security. Springer, Wiesbaden, S 1–13

Mashiane T, Kritzinger E (2019) Cybersecurity behaviour: a conceptual taxonomy. In: Blazy O, Yeun CY (Hrsg) Information security theory and practice. Springer, Cham, S 147–156
McFadzean E, Ezingeard J-N, Birchall D (2011) Information assurance and corporate strategy: a Delphi study of choices, challenges, and developments for the future. Inf Syst Manag 28:102–129. https://doi.org/10.1080/10580530.2011.562127
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen, Digitale Hochschule NRW (2023) Vereinbarung zur Informationssicherheit an den Hocschulen (Vzl)
Ministerium für Kultur und Wissenschaften des Landes Nordrhein-Westfalen (2024) Vereinbarung zur Cybersicherheit (VzC). In: Cybrsicherheit. https://www.mkw.nrw/themen/wissenschaft/wissenschaftspolitik/cybersicherheit. Zugegriffen: 5. Aug. 2025
NIS2 Directive: securing network and information systems | Shaping Europe's digital future (2022) https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. Zugegriffen: 5. Aug. 2025
Parsons K, McCormac A, Butavicius M et al (2014) Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur 42:165–176. https://doi.org/10.1016/j.cose.2013.12.003
Rogers RW (1975) A protection motivation theory of fear appeals and attitude change1. J Psychol 91:93–114. https://doi.org/10.1080/00223980.1975.9915803
Schein EH (2017) Organizational culture and leadership, 5. Aufl. Wiley, Hoboken
Scholl M, Schuktomow R, v. Tippelskirch H et al (2023) AWARENESS FORUM 2023
Schuktomow R, von Tippelskirch H, Scholl M (2023) Informationssicherheit in den Arbeitsalltag nachhaltig integrieren https://doi.org/10.18420/INF2023_16
Schütz AE (2018) Information security awareness: it's time to change minds! Proceedings of International Conference on Applied Informatics Imagination, Creativity, Design, Development-ICDD.
secaware.nrw (2025) https://secaware.nrw/. Zugegriffen: 11. Aug. 2025
Selbstlernakademie › secaware.nrw (2023) https://secaware.nrw/selbstlernakademie/. Zugegriffen: 9. Jan. 2026
Shank E, Tang H, Morris W (2024) Motivation in online course design using self-determination theory: an action research study in a secondary mathematics course. Educ Technol Res Dev. https://doi.org/10.1007/s11423-024-10410-9
Stanton B, Theofanos MF, Prettyman SS, Furman S (2016) Security fatigue. IT Prof 18:26–32. https://doi.org/10.1109/MITP.2016.84
Tschakert KF, Ngamsuriyaroj S (2019) Effectiveness of and user preferences for security awareness training methodologies. Heliyon 5:e2010. https://doi.org/10.1016/j.heliyon.2019.e02010
Tsohou A, Karyda M, Kokolakis S, Kiountouzis E (2015) Managing the introduction of information security awareness programmes in organisations. Eur J Inf Syst 24:38–58. https://doi.org/10.1057/ejis.2013.27
Uchendu B, Nurse JRC, Bada M, Furnell S (2021) Developing a cyber security culture: current practices and future needs. Comput Secur 109:102387. https://doi.org/10.1016/j.cose.2021.102387
Wang Y, Wang H, Wang S et al (2024) A systematic review and meta-analysis of self-determination-theory-based interventions in the education context. Learn Motiv 87:102015. https://doi.org/10.1016/j.lmot.2024.102015
Wiarda J-M (2025) Nicht nur Berlin kürzt bei den Hochschulen: Hier sparen Bayern, Hessen und NRW an Forschung und Lehre – und hier wird investiert. Der Tagesspiegel Online
Witte J (2025) Kürzungen Uni Bielefeld: Dieser Studiengang muss schon jetzt mit Weniger auskommen. https://www1.wdr.de/nachrichten/westfalen-lippe/protest-kuerzungen-uni-bielefeld-104.html. Zugegriffen: 12. Aug. 2025
Zwilling M, Klien G, Lesjak D et al (2022) Cyber security awareness, knowledge and behavior: a comparative study. J Comput Inf Syst 62:82–97. https://doi.org/10.1080/08874417.2020.1712269