Entwicklung, Evaluation und Distribution einer Selbstlernakademie zum Thema IT-Sicherheit

Miriam Naß[1], Tabea Dobbrunz[2], Sina Warmer[2], Andreas Harrer[2] und Norbert Pohlmann[1]

Abstract: Im Rahmen des vom Ministerium für Kultur und Wissenschaft des Landes NRW und von der Digitalen Hochschule NRW (DH.NRW) geförderten Projekts SecAware.nrw wurde eine Selbstlernakademie zum Thema IT-Sicherheit entwickelt. Mit dem Ziel Bewusstsein zu schaffen, stellt dieses Lernangebot eine Präventionsmaßnahme für die vermehrt stattfindenden Cyber-Angriffe auf Hochschulen dar. Das Angebot setzt dabei auf ein multimediales didaktisches Konzept, bestehend aus informativ aufbereiteten und zur Exploration anregenden Elementen. Ergebnisse aus Evaluationen deuten darauf hin, dass die Zielgruppen eine Mischung aus Videos, Fachtexten und interaktiven Elementen als effektiv und motivierend wahrnehmen. Die Verbreitung der Online-Selbstlernakademie unter Hochschulangehörigen erfolgt aktuell durch eine zusätzliche Kommunikationsstrategie, welche auf eine maximale Reichweite und eine starke Nutzendenbindung abzielt.

Keywords: Selbstlernkurs, IT-Sicherheit, Multimediales Lernangebot, Laborstudie

1 Einleitung

Cyberkriminelle bevorzugen Universitäten und Hochschulen als Angriffsziele aufgrund der umfangreichen, sensiblen Daten, wie die „Jahresberichte 2022 und 2023 des Bundesamtes für Sicherheit in der Informationstechnik (BSI)“ belegen [Bu]. Besonders im Jahr 2023 zeigt sich der Fokus auf wissenschaftliche Einrichtungen: Von 23 registrierten Ransomware-Attacken im Bildungssektor zielten 13 auf Hochschulen und Forschungseinrichtungen ab. Die fortschreitende Digitalisierung erhöht die Herausforderungen für diese Institutionen und die ansässige Hochschulgemeinschaft, da stetige Anpassungen an neue Technologien und das Internet notwendig sind.

Der „Faktor Mensch“ wird als entscheidender Risikofaktor innerhalb der IT-Sicherheit identifiziert. Faktoren wie Zeitmangel, fehlende Lernmöglichkeiten und unzureichendes Fachwissen erhöhen nicht nur das Risiko unbefugter Zugriffe durch externe Angreifende, sondern fördern auch unbeabsichtigt riskantes Verhalten seitens der Nutzenden. Cyberkriminelle nutzen diese menschlichen Schwachstellen zunehmend aus. Daher besteht die Notwendigkeit einer stetigen Überprüfung und Anpassung der Sicherheitsstrategien, um den dynamischen Cyberbedrohungen effektiv entgegentreten zu können.

1 Westfälische Hochschule Gelsenkirchen, Institut für Internet-Sicherheit, Neidenburger Straße 43, 45897 Gelsenkirchen, Deutschland, miriam.nass@w-hs.de; pohlmann@internet-sicherheit.de, https://orcid.org/0009-0007-6221-7327

2 Fachhochschule Dortmund, Institut für Digitalisierung von Arbeits- und Lebenswelten, Otto-Hahn-Straße 23 & 27, 44227 Dortmund, Deutschland, tabea.dobbrunz@fh-dortmund.de; sina.warmer@fh-dortmund.de; andreas.harrer@fh-dortmund.de, https://orcid.org/0009-0001-1076-7964

doi:10.18420/delfi2024_37

Diesen Herausforderungen begegnet das Projekt SecAware.nrw mit einem speziell auf Studierende und akademisches Personal zugeschnittenen Selbstlernangebot in deutscher und englischer Sprache. Das Angebot zielt darauf ab, IT-Kompetenzen und Cyber-Sicherheitsbewusstsein im akademischen Umfeld zu stärken. Die partizipative Entwicklungsmethode („User Centered Design“) und kontinuierliche qualitative Evaluationen gewährleisten die Relevanz und Effektivität des Angebots.

2 Related Work

Die digitale Bildungslandschaft entwickelt sich durch Initiativen, die IT-Kompetenzen und Cybersecurity-Bewusstsein fördern, stetig weiter. Dieses Kapitel stellt drei aktuelle Bildungsprogramme vor:

Erstens, **DIGI-V.nrw**, initiiert von der DH-NRW, zielt darauf ab, die digitalen Kompetenzen von Personal in Hochschulverwaltungen zu fördern. Es bietet Fortbildung und Vernetzung mit einem Fokus auf praktische und theoretische Kenntnisse zur Integration neuer Technologien in den Arbeitsalltag, unterstützt durch ein Konzept bestehend aus Fachtexten und Quizzen [Di]. Zweitens, der **Digitale Führerschein (DiFü)**, unterstützt vom Bundesministerium des Innern und für Heimat (BMI), ist ein Projekt von Deutschland sicher im Netz e.V., das digitales Grundlagenwissen und Sicherheit im Umgang mit Technologien vermittelt. Durch ein interaktives System profitieren Menschen aller Altersgruppen [De]. Drittens, die **IT-Grundschutz-Schulungen des BSI** zielen darauf ab, ein angemessenes Sicherheitsniveau für Organisationen und Einzelpersonen herzustellen [Bu18]. Alle drei Angebote besitzen Möglichkeiten zur Selbstüberprüfung und weisen modulare Konzepte auf.

Obwohl diese Programme bereits Beiträge zur digitalen Bildung leisten, adressieren sie allgemeine Zielgruppen oder spezifische Berufsgruppen. Es mangelt jedoch an praxisbezogenen Angeboten, die auf die Förderung von Cyber- und IT-Sicherheit besonders gefährdeter Personen im Hochschulkontext fokussiert sind. Damit sind als Zielgruppen die Professorenschaft, Studierende und wissenschaftliche Mitarbeitende bisher nicht angesprochen.

Das Projekt SecAware.nrw hat die maßgeschneiderte Ausrichtung auf diese Zielgruppen durch ein kostenfreies Angebot zum Ziel. Das umfangreiche Lernangebot zeichnet sich durch eine stringente Logik aus und kann nach Bedarf flexibel modular eingesetzt werden.

3 Didaktisches Design

Bei der Konzeption wurden besonders frühere Arbeiten nach Bergmann et al. [Be21] einbezogen. Bergmann et al. entwickelten die Lernplattform *FALEDIA*, die speziell auf die Bedürfnisse von Lehramtsstudierenden zugeschnitten ist und diesen dabei hilft, ihre Fähigkeiten in der Diagnose und Förderung für die Primarstufe zu entwickeln. Diese Arbeit diente als Grundlage für die Entwicklung des didaktischen Konzepts.

Um höhere Lernzielebenen [AK01] und damit eine kritische Reflektion und nicht nur die Kenntnis von Fakten erreichen zu können, wurde Anwendung und Analyse der Inhalte durch Aktivitäten der Lernenden unterstützt. Dazu dienen interaktive Elemente, die auch die Selbstwirksamkeit und Motivation fördern [Ke18]. Impulse zur Gestaltung und Implementierung der interaktiven Elemente wurden aus Bayrak et al. [BRS21] aufgenommen, die in ihrem Beitrag ein interaktives E-Mail-Interface für Lernspiele zur Sensibilisierung gegen Phishing-Angriffe vorstellten.

Bei der Konzeption der Lehrinhalte stellt besonders die Heterogenität innerhalb der und zwischen den Zielgruppen eine Herausforderung dar. Die multimedialen Lehrinhalte und redundant gestalteten *Videos* sowie *Fachtexte* sprechen daher ein möglichst breites Publikum an, unterstützen unterschiedliche Vorgehensweisen und sorgen neben Untertiteln für Barrierefreiheit. Da es sich um ein freiwilliges Lernangebot handelt, wurden Fachtexte in einfacher Sprache verfasst und Videos mit maximaler Länge von fünf Minuten kurz und prägnant gehalten [Da20; GKR14], um die Motivation zu erhalten.

Das Lernangebot unterteilt sich in insgesamt acht *Module* (Stand: März 2024): Ein Einleitungsmodul, welches durch ein fiktives Beispiel Interesse weckt und sieben inhaltliche Module, z.B. Social Engineering, Urheberrecht und Lizenzen. Diese umfassen ein bis vier Themenseiten und je ein abschließendes *Modulquiz*.

Abb. 1: Interaktives Element, in dem Lernende personenbezogene Informationen aus einem Social Media Feed sammeln und beispielhaft für die Formulierung eines Phishing Angriffs nutzen

Animierte Videos stellen die Themen vor und fassen die wesentlichen Aspekte unter den Rubriken „`BE AWARE`“ und „`BE SMART`“ zusammen. Im Anschluss werden die Inhalte nochmals als Fachtext dargeboten. Bei ausgewählten Themen folgt mit „`BE ACTIVE`“ ein zur Exploration anregendes Element in Form einer interaktiven Animation oder einer kurzen Aufgabe zur Selbstüberprüfung (siehe Abb. 1). Am Ende einer Seite werden die wichtigsten Punkte sowie weiterführende Links zur Vertiefung des Themas aufgelistet. Der didaktische Aufbau aus informierenden Inhalten und anschließenden interaktiven Elementen folgt den Erkenntnissen aus Bergmann et al. [Be21].

Im abschließenden Modulquiz können die Lernenden ihr Wissen mittels einfachen Single- und Multiple-Choice-Fragen sowie Zuordnungs- oder Freitextaufgaben überprüfen. Nach Abschluss wird den Lernenden visualisiert, wie viel Prozent der Fragen richtig beantwortet worden sind. Das Quiz kann dabei beliebig oft wiederholt werden.

4 Produktionsprozess und Umsetzung

Der auf Kommunikation und Journalismus spezialisierte Teil des Projektteams erstellt *Skripte* für Lernvideos und Fachtexte basierend auf der Grundlage geprüfter Quellen und sorgfältiger Recherche. Die Redaktion verfasst die Skripte, welche iterativ für die Videoproduktion angepasst und von externen Fachexperten überprüft werden. Die finalen Versionen werden von professionellen Sprechenden aufgenommen. Komplexe Sicherheitskonzepte werden über *Videos* mit fiktiven Szenarien erklärt, wobei Begriffe wie „Socialgram“ (siehe Abbildung 1) verwendet werden, um konkrete Plattformen nicht zu exponieren und mit ihren etwaigen Sicherheits- und Datenschutzproblemen in Bezug zu stehen. Zudem werden unterstützende *Grafiken* zur Veranschaulichung des Lernmaterials erstellt.

Die Entwicklung des E-Learning-Contents erforderte insgesamt 69 Personenmonate, also 9.889,77 Arbeitsstunden. Diese wurden auf 21 Themenseiten aufgeteilt, was einen Durchschnitt von etwa 470,94 Stunden pro Thema (ca. 20 Arbeitstagen) entspricht. Das stimmt mit früheren Schätzungen, wie Chapmans Durchschnitt von 490 Stunden für komplexe E-Learning-Module überein. Angesichts der durchschnittlichen Nutzungsdauer von 20-25 Minuten pro Thema ergibt sich ein Verhältnis von Produktionszeit zu Nutzungszeit von 1129,74 bis 1413,06. Laut Chapman kann für komplexe Projekte einen Faktor ab 716 entstehen [Ch10]. Durch die ermittelten Faktoren in diesem Projekt wird der hohe Aufwand für den Produktionsprozess unterstrichen.

Für die iterative Umsetzung der Lernplattform inklusive der Quizze, wurde das Autorentool *Articulate Rise 360*[3] verwendet, welches die kollaborative Erstellung optisch ansprechender E-Learning-Kurse vereinfacht. Darüber hinaus ermöglicht es den Export als SCORM-Modul[4]. Die eingesetzte Software ermöglicht zudem schnell eine Vorschau des Kurses zu erstellen, welche externen Personen für eine Revision zur Verfügung gestellt werden kann.

Mithilfe der Zusatzsoftware *Articulate Storyline 360*[5] wurden die interaktiven Elemente erstellt. Diese werden in Form von Folienpräsentationen designt, welche dabei diverse Storypfade abbilden können. Durch eine Vielzahl an Events können Ebenen auf den Folien angezeigt oder ausgeblendet werden. Es ist möglich den Folien Komponenten zur Wissensüberprüfung hinzuzufügen, die das Ergebnis an ein *Lernmanagementsystem (LMS)* übermitteln.

3 https://www.articulate.com/360/rise/
4 E-Learning-Standard SCORM: https://scorm.com/
5 https://www.articulate.com/360/storyline/

5 Evaluation

Die SecAware.nrw-Selbstlernakademie wurde über einen Zeitraum von zwei Jahren kontinuierlich evaluiert. In regelmäßigen Abständen erfolgte die Bereitstellung von Inhalten für Expertenfeedback an die Chief Information Security Officers (CISOs) der Hochschulen in NRW. Darüber hinaus wurden zwei Laborstudien mit zehn beziehungsweise zwanzig Teilnehmenden durchgeführt. Die Studien umfassten außerdem die Beantwortung von Fragebögen sowie die Durchführung von Interviews. Die erste Studie fokussierte sich auf Videos und das didaktische Konzept. Im Gegensatz dazu zielte die zweite Studie auf die Bewertung des überarbeiteten Konzepts, der resultierenden Selbstlernakademie sowie die interaktiven Elemente ab. Das Feedback der CISOs und der Studienteilnehmenden fließt beständig in die Weiterentwicklung der Selbstlernakademie ein.

Die an der Laborstudie teilnehmenden Personen wurden gebeten, unter Anwendung der *Think-Aloud-Methode* jeweils drei ausgewählte Themenseiten mit interaktiven Elementen sowie ein Quiz zu bearbeiten. Im Anschluss haben die Teilnehmenden die Gebrauchstauglichkeit sowie ihre persönliche Erfahrung mit der Selbstlernakademie evaluiert. Eingesetzt wurden hierfür der reduzierte *User Experience Questionnaire (UEQ-S)* [SHT17] sowie vier Subskalen des *Intrinsic Motivation Inventory (IMI)* [RMK83; Ry82]. Des Weiteren schätzten die Teilnehmenden ihre Erfahrung mit dem Thema IT-Sicherheit und dem Umgang mit Lernplattformen ein. Während viele der Teilnehmenden ihre Erfahrung mit Lernplattformen eher hoch bewerteten, sind die Erfahrungen mit dem Thema IT-Sicherheit gemischt.

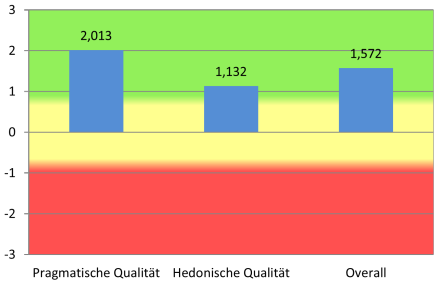

Abb. 2: Bewertung der Usability (UEQ-S)

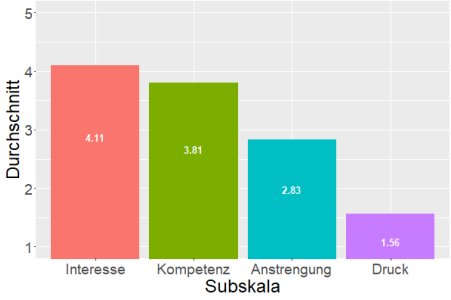

Abb. 3: Bewertung mittels IMI

Die Gebrauchstauglichkeit der Selbstlernakademie wurde durch den UEQ-S mit einem Wert von 1, 572, wie Abbildung 2 dargestellt, insgesamt sehr gut bewertet. Dabei wurde die reine Funktionalität durch die *pragmatische Qualität* (PQ = 2, 013) höher bewertet, als das empfundene Vergnügen durch die *hedonische Qualität* (HQ = 1, 132).

Der IMI ergab eine hohe Bewertung auf der Subskala „Interesse/Vergnügen“, welche mit der intrinsischen Motivation in Verbindung gebracht wird (Siehe Abb. 3). Auch die Skala „wahrgenommene Kompetenz“ wurde als gut bewertet und gilt als positiver Faktor auf die intrinsische Motivation. Der negative Faktor „Druck/Anspannung“ wurde dabei als niedrig evaluiert. Das Ergebnis der Subskala „Anstrengung/Wichtigkeit“ liegt im mittleren Bereich.

6 Distribution

Das Lernangebot steht auf der `Webseite` (Open Access) zur Verfügung und kann für die Integration in LMS wie Moodle oder ILIAS heruntergeladen werden. Für eine effektive Verbreitung unter Hochschulangehörigen sind jedoch verstärkte Anstrengungen in den Bereichen Marketing, Kommunikation und Netzwerkbildung erforderlich, um eine optimale Reichweite und Nutzendenbindung zu erreichen. Als Teil dieser Bemühungen wurden bereits erste Implementierungsschritte unternommen:

- **Öffentlichkeitsarbeit und Social Media:** Um die Aufmerksamkeit innerhalb der Hochschulgemeinschaft zu erhöhen, wurden zwei Pressemitteilungen und ein Instagram-Video veröffentlicht, welche das Angebot breit kommunizieren und zielgruppenspezifisch zugänglich machen.
- **Vorträge, Seminare und Konferenzen:** Durch Teilnahme an Veranstaltungen und Workshops, die die Anwendung der Plattform demonstrieren, wurde ein erster Eindruck vermittelt und ein direkter Austausch mit Interessierten gefördert.
- **Kooperationen:** Die Einbindung von Stakeholdern, wie beispielsweise CISOs als Multiplikatoren, verstärken die Reichweite der Inhalte.

Die Kombination verschiedener Formate zielt darauf ab, Reichweite in der Distribution für SecAware.nrw zu realisieren. Der Erfolg dieser Maßnahmen wird mittels technischer Reporting-Ansätze sowie weiterführender Evaluationsaktivitäten überwacht und bewertet.

7 Fazit und Ausblick

Der hohe Arbeitsaufwand bei der Entwicklung und Umsetzung der Lernmaterialen resultieren in einer Selbstlernakademie, die eine insgesamt positiv bewertete Gebrauchstauglichkeit und wahrgenommene intrinsische Motivation aufweist. Der gemessene zeitliche Aufwand unterstreicht die Notwendigkeit einer guten Projektplanung bei der Erstellung von E-Learning-Kursen. Besonders bei der Videoproduktion mit externen professionellen Sprechenden ist ein komplexer Prozess zu durchlaufen. Der Einsatz von Autorentools für die Generierung von Modulen kann sich dagegen positiv auf die benötigte Zeit auswirken, da die Einhaltung des SCORM-Standards sowie eine einheitliche Gestaltung größtenteils durch das Tool gewährleistet wird. Jedoch sind hier Limitationen in der Umsetzungsfreiheit sowohl im Design (Farb-, Symbol- und Dialoggestaltung) als auch in der Erhebung von Nutzendendaten zur Analyse von Lernaktivitäten zu beachten. Darüber hinaus wird die Anpassbarkeit durch Dritte im Sinne von Open Educational Ressources beeinträchtigt.

Da das Thema IT-Sicherheit ein sich stetig änderndes breites Feld darstellt, wird die Selbstlernakademie innerhalb der nächsten drei Jahre kontinuierlich aktualisiert und um neue Module erweitert. Gleichzeitig wird die Wirksamkeit des Angebots quantitativ evaluiert, um die Nutzungserfahrung zu verbessern.

Literaturverzeichnis

[AK01] Anderson, L. W.; Krathwohl, D. R., Hrsg.: A Taxonomy for Learning, Teaching, and Assessing. A Revision of Bloom's Taxonomy of Educational Objectives. Allyn & Bacon, New York, 2001, ISBN: 978-0801319037.

[Be21] Bergmann, A.; Dobbrunz, T.; Harrer, A.; Huethorst, L.; Walter, D.; Gutscher, A.; Selter, C.: FALEDIA: Eine Lernplattform für Lehramtsstudierende zum Erwerb von Diagnose- und Förderfähigkeit. 2021.

[BRS21] Bayrak, D.; Röpke, R.; Schroeder, U.: Konzeption und Entwicklung eines interaktiven E-Mail- Interface für Anti-Phishing Lernspiele. 2021.

[Bu] Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2023, Bundesamt für Sicherheit in der Informationstechnik, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=132646, Stand: 07. 03. 2024.

[Bu18] Bundesamt für Sicherheit in der Informationstechnik (BSI): Online-Kurs IT-Grundschutz - Druckversion. S. 1–103, 2018, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/onlinekurs2018.pdf?__blob=publicationFile&v=1, Stand: 12. 03. 2024.

[Ch10] Chapman, B.: How Long Does it Take to Create Learning? Chapman Alliance, 2010, URL: https://www.cedma-europe.org/newsletter%20articles/misc/How%20long%20does%20it%20take%20to%20develop%20training%20by%20Brian%20Chapman%20(Sep%2010).pdf.

[Da20] Dart, S.: Khan-Style Video Engagement in Undergraduate Engineering: Influence of Video Duration, Content Type and Course. In: Proceedings of the 31st Annual Conference of the Australasian Association for Engineering Education (AAEE 2020). Conference Name: AAEE - Annual Conference of Australasian Association for Engineering Education Meeting Name: AAEE - Annual Conference of Australasian Association for Engineering Education, Engineers Australia, Australia, 2020, URL: https://www.aaee2020.com.au/wp-content/uploads/2020/11/AAEE2020_paper_4.pdf, Stand: 14. 03. 2024.

[De] Deutschland sicher im Netz: Lernzentrale, Digitalführerschein (DiFü), URL: https://difue.de/lernzentrale/, Stand: 12. 03. 2024.

[Di] Digi-V.dh.nrw: digi-v.dh.nrw, URL: https://digi-v.dh.nrw/, Stand: 11. 03. 2024.

[GKR14] Guo, P. J.; Kim, J.; Rubin, R.: How video production affects student engagement: an empirical study of MOOC videos. In: Proceedings of the first ACM conference on Learning @ scale conference. L@S 2014: First (2014) ACM Conference on Learning @ Scale. ACM, Atlanta Georgia USA, S. 41–50, 2014, ISBN: 978-1-4503-2669-8, DOI: 10.1145/2556325.2566239, URL: https://dl.acm.org/doi/10.1145/2556325.2566239, Stand: 14. 03. 2024.

[Ke18] Kerres, M.: Mediendidaktik: Konzeption und Entwicklung digitaler Lernangebote. Publication Title: Mediendidaktik, De Gruyter Oldenbourg, 2018, ISBN: 978-3-11-045683-7.

[RMK83] Ryan, R. M.; Mims, V.; Koestner, R.: Relation of reward contingency and interpersonal context to intrinsic motivation: A review and test using cognitive evaluation theory. Journal of Personality and Social Psychology 45 (4), Place: US Publisher: American Psychological Association, S. 736–750, 1983, ISSN: 1939-1315, DOI: 10.1037/0022-3514.45.4.736.

[Ry82] Ryan, R. M.: Control and information in the intrapersonal sphere: An extension of cognitive evaluation theory. Journal of Personality and Social Psychology 43 (3), Place: US Publisher: American Psychological Association, S. 450–461, 1982, ISSN: 1939-1315, DOI: 10.1037/0022-3514.43.3.450.

[SHT17] Schrepp, M.; Hinderks, A.; Thomaschewski, J.: Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S). International Journal of Interactive Multimedia and Artificial Intelligence 4, S. 103–108, 2017, DOI: 10.9781/ijimai.2017.09.001.