ALARM
Awareness Labor KMU
Informationssicherheit

Schlussbericht des Projekts
„Awareness Labor KMU (ALARM) Informationssicherheit“:

Neue Wege für mehr Informationssicherheit in deutschen Klein- und mittelständischen Unternehmen

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Margit Scholl (Hrsg.)

Schlussbericht

des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“:

Neue Wege für mehr Informationssicherheit in deutschen Klein- und mittelständischen Unternehmen

Bibliographische Informationen der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zitierung:
Scholl, M. (2024). Schlussbericht des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“: Neue Wege für mehr Informationssicherheit in deutschen Klein- und mittelständischen Unternehmen. Wildau: TH Wildau.

Imprint
Schlussbericht
des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“:
Neue Wege für mehr Informationssicherheit in deutschen Klein- und mittelständischen Unternehmen

https://alarm.wildau.biz/

1. Auflage März 2024

Printed in Germany.

Technische Hochschule Wildau
Hochschulring 1
15745 Wildau

ISBN: 978-3-949639-09-8

Schlussbericht

des Projekts
„Awareness Labor KMU (ALARM) Informationssicherheit“:

Neue Wege für mehr Informationssicherheit
in deutschen Klein- und mittelständischen Unternehmen

Projektlaufzeit: 01.10.2020 – 30.09.2023 /
kostenneutrale Verlängerung (KNV) 01.10.2023 – 31.03.2024

Margit Scholl

Projektwebseite:	**Peter Koppatz**
Layout und Design:	**Olesja Mujkic**
Korrektorat:	**Bernhard Zientek**
Laborunterstützung:	**Peter Ehrlich**

Forschungsgruppe
„Informationssicherheit & Awareness (Oktober 2023 – März 2024)“
an der Technischen Hochschule (TH) Wildau
https://wildau.biz/

Das diesem Werk zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MS19002A gefördert.

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart
978-3-949639-09-8	Schlussbericht

3a. Titel des Projekts
Projekt „Awareness Labor KMU (ALARM): Interaktiv-erlebbare Personalentwicklung für mehr Informationssicherheit und organisationsweite Sicherheitsanalysen in KMU“ [„Awareness Labor KMU (ALARM) Informationssicherheit“]

3b. Titel des Berichts
Margit Scholl (Hrsg.)(2024). **Schlussbericht des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“: Neue Wege für mehr Informationssicherheit in deutschen Klein- und mittelständischen Unternehmen.** Wildau: TH Wildau

3b. Titel der zugrundeliegenden Publikation
Margit Scholl (Hrsg.)(2024a). Neue Wege für mehr Informationssicherheit in KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit. Frankfurt/M.: Buchwelten Verlag, 2024, 234 Seiten.

4a. Autorin des Berichts (Name, Vorname(n))
Scholl Margit

4b. Autorinnen und Autoren der zugrundeliegenden Publikation (Name, Vorname(n))
Scholl, M., Schuktomow, R., von Tippelskirch, H., Prott, F., Koppatz, P., Pokoyski, D., Küchler, U. & Vogt, M.

5. Abschlussdatum des Vorhabens
31.03.2024

6. Veröffentlichungsdatum des Berichts
31.03.2024

7. Form des Berichts / der Publikation
PDF / Buch

8. Durchführende Institution(en) (Name, Adresse)

Technische Hochschule Wildau
Prof. Dr. Margit Scholl

Hochschulring 1
15745 Wildau

9. Ber.Nr. Durchführende Institution
13410527,
Schlussbericht „ALARM“ final, TH Wildau, 2024

10. Förderkennzeichen
01MS19002A

11a. Seitenzahl Bericht
Insgesamt 50

13. Fördernde Institution (Name, Adresse)

Bundesministerium für
Wirtschaft und Klimaschutz (BMWK)

53107 Bonn

11b. Seitenzahl Publikation
234 Seiten

Weitere Publikationen zum Projekt „ALARM Informationssicherheit“ siehe Kapitel 4 des Berichts (Anlagen)

12. Literaturangaben
Anlage 4.1; insgesamt 33 wiss. Veröffentlichungen

14. Tabellen
2 als Abbildungen

15. Abbildungen
Insgesamt 28

16. Zusätzliche Angaben
Forschungsgruppe „Informationssicherheit & Awareness (2023/2024)“
von Professorin Dr. Margit C. Scholl
an der Technischen Hochschule (TH) Wildau

Siehe
https://wildau.biz/

Ebenso
https://alarm.wildau.biz/
https://www.th-wildau.de/scholl/
https://en.th-wildau.de/index.php?id=23836

17. Vorgelegt bei (Titel, Ort, Datum)

DLR Projektträger
Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
Matthias Hanschke
Heinrich-Konen-Straße 1
53227 Bonn

18. Kurzfassung nach Margit Scholl (Hrsg.) (2024a):

Der Begriff Informationssicherheit bezieht sich auf den Schutz von Informationen jeglicher Art und Herkunft und geht über die oft – trotz ihrer Verschiedenheit – synonym genutzten Begriffe IT-Sicherheit, Cyber-Sicherheit und Datenschutz hinaus. Gefährdungen existieren durch menschliche Fehlhandlungen, organisatorische Mängel, vorsätzliche Handlungen, technisches Versagen oder höhere Gewalt. Führungskräfte und Mitarbeitende der Unternehmen sollten daher gegenüber technischen und organisatorischen Maßnahmen (TOM), mit denen den Gefährdungen angemessen begegnet werden kann, aufmerksam sein. Dies setzt in den Unternehmen eine aktive Personalentwicklung zur Informationssicherheit und ein umfangreiches Risikomanagement hinsichtlich der betrieblichen Prozesse voraus.

Aufgrund der zeitlichen Verzögerung zwischen zum Beispiel einem Cyberangriff und seinen betrieblichen Auswirkungen können zudem langfristige Konsequenzen für ein Unternehmen resultieren, so dass eine kontinuierliche Verbesserung des betrieblichen Informationssicherheitsmanagements eine entscheidende Rolle bei der Reduzierung von Sicherheitsrisiken spielt. Dieser Ansatz wurde auch im Rahmen des hier dargestellten Projekts „Awareness Labor KMU (ALARM) Informationssicherheit" mit dem Fokus auf „Hilfe zur Selbsthilfe" für kleine und mittlere Unternehmen (KMU) verfolgt. Dieses praxisorientierte Forschungsprojekt liefert mit seinen Ergebnissen einen fundierten Beitrag für eine aktive Personalentwicklung und nachhaltige Sensibilisierung. Das Projekt und seine Ergebnisse sind von besonderer Bedeutung für die Erhöhung des Sicherheitsniveaus in deutschen KMU, da Untersuchungen der Situation immer wieder zeigen, dass trotz der fortschreitenden Digitalisierung das Bewusstsein für IT-Sicherheit in Deutschland noch mangelhaft ist. Selbst wenn die Risikowahrnehmung gewachsen ist, fehlt es an einer umfassenden Umsetzung verschiedener Informationssicherheitsmaßnahmen, die nicht nur technischer Natur sein dürfen.

Aktuelle Studien zeigen, dass in den deutschen KMU inzwischen zwar technische Vorkehrungen zur Risikoreduzierung getroffen werden, allerdings kein nennenswerter Anstieg in organisatorischen Maßnahmen für Informationssicherheit – inklusive Sensibilisierung und Schulung von Personal – zu verzeichnen ist und zudem nur ein Drittel der befragten Unternehmen über einen Notfallplan verfügt. Immer mehr rückt der Mensch ins Zentrum des Geschehens zur Erhöhung der Informationssicherheit. Das Projekt „ALARM Informationssicherheit" basiert auf dem Grundsatz: „Digitalisierung nur mit Informationssicherheit. Informationssicherheit nur mit Awareness."

Das Projekt erfüllt trotz widriger Umstände infolge der Corona-Pandemie seine Ziele: Basierend auf Aussagen von deutschen KMU durch Interviews (veröffentlichte Studien 1, 2, 3) und Online-Umfragen (veröffentlichte Reports 1 und 3) wurden sieben analoge Lernszenarien, sieben digitale Serious Games und sieben niederschwellige Sicherheitskonzepte für KMU konzipiert, in der Praxis erprobt und mit Projektende kostenfrei für die nicht-kommerzielle Nutzung zur Verfügung gestellt. Darüber hinaus hat das Projektteam noch weitere Ergänzungen innerhalb einer sehr aktiven Öffentlichkeitsarbeit zur Verfügung gestellt: ein digitaler Selbsttest für Mitarbeitende, ein zusätzliches Serious Password-Hacking-Game sowie etliche deutsche und englische wissenschaftliche Veröffentlichungen.

In der kostenneutralen Verlängerung (von Oktober 2024 bis März 2024) konnte die Projektdokumentation auf Deutsch als Buch finalisiert und veröffentlicht werden (s.o.). Darüber hinaus wurden weitere Kontakte geknüpft, Anfragen beantwortet und bei etlichen öffentlich wirksamen Events für KMU die Materialien umfänglich vorgestellt. Zudem wurden 2024 fünf neue Podcasts konzipiert und in Auftrag gegeben, damit die Veröffentlichungen der Projektergebnisse auch international bekannt gemacht werden. Siehe **https://alarm.wildau.biz**
19. Schlagwörter Informationssicherheitsbewusstsein, Awareness, Training, Serious Games, analoge Lernszenarien, digitale Spiele, niederschwellige Sicherheitskonzepte, erprobte Materialien für KMU

20. Verlag	21. Preis des Berichts
PDF, TH Wildau, Download unter: https://alarm.wildau.biz/	kostenfrei

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication)
978-3-949639-09-8	Final report

3. title of this report

Margit Scholl (Hrsg.)(2024). **Schlussbericht des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit": Neue Wege für mehr Informationssicherheit in deutschen Klein- und mittelständischen Unternehmen.** Wildau: TH Wildau

4. background of this publication	5. end of project
a) Scholl Margit (Ed.)(2024). Neue Wege für mehr Informationssicherheit in KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit. Frankfurt/M.: Buchwelten Verlag, pp. 234. b) Scholl, M. (2024). Résumé of the Gamified Increase in Security Awareness in German Small and Medium-Sized Businesses after Three Years' Practice of "ALARM Information Security" doi:10.13140/RG.2.2.13519.29600 c) Scholl, M. (2024). Summary of the project documentation "Awareness Lab SME (ALARM) Information Security" doi:10.13140/RG.2.2.20336.64002/1	31.03.2024
	6. publication date 31.03.2024
	7. form of this publication Free PDF
8. performing organization(s) (name, address) University of Applied Sciences Wildau Technische Hochschule Wildau Prof. Dr. Margit Scholl Project "ALARM Information Security" Hochschulring 1 15745 Wildau	9. originator's report no. 13410527, Final report "ALARM", TH Wildau, 2024
	10. reference no. 01MS19002A
	11. no. of pages 50
12. sponsoring agency (name, address) Bundesministerium für Wirtschaft und Klimaschutz (BMWK) 53107 Bonn	13. no. of references 33 publications (see section 4.1 of the report)
	14. no. of tables 2 as figures
	15. no. of figures In sum 28

16. supplementary notes

For further publications on the "ALARM Information Security" project, see Appendix 1.

17. presented at (title, place, date)

DLR Projektträger
Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
Matthias Hanschke
Heinrich-Konen-Straße 1
53227 Bonn

18. abstract

The term information security refers to the protection of information of all types and origins and goes beyond the terms IT security, cybersecurity, and data protection, which, despite their differences, are often used synonymously. Information security threats may arise from human error, organizational deficiencies, intentional actions, technical failure, or force majeure.

Managers and employees of companies should therefore be attentive to technical and organizational measures (TOM) that can be used to adequately address the risks. This requires active personnel development focused on information security and extensive risk management with regard to operational processes.

The "ALARM Information Security" project is based on the principle "Digitization only with information security. Information security only with awareness."

18. abstract

The project met its goals despite the adverse circumstances resulting from the Covid pandemic. Based on statements from German SMEs gathered from interviews (published studies 1, 2, 3) and online surveys (published reports 1 and 3), seven analog learning scenarios, seven digital serious games, and seven low-threshold security concepts for SMEs were designed, tested in practice, and made available free of charge for non-commercial use at the end of the project. In addition, the project team has made other additions available as part of a very active public relations effort: a digital self-test for employees, an additional serious password-hacking game, and a number of German and English scientific publications.

During the cost-neutral extension (October 2023 – March 2024), the project documentation was finalized and published in German as a book (see above). In addition, further contacts were made, inquiries were answered, and the materials were presented in detail at a number of public events for SMEs. Five new podcasts were commissioned in 2024 so that the project results can also be made known internationally.

For project material, see https://alarm.wildau.biz

19. keywords

Information security awareness, training, analog and digital serious games, analog low-threshold security concepts for SMEs and digital additions

20. publisher	21. price of this publication
PDF, TH Wildau Download at: https://alarm.wildau.biz/	free of charge

https://alarm.wildau.biz

Schlussbericht

„Awareness Labor KMU (ALARM): Interaktiv-erlebbare Personalentwicklung für mehr Informationssicherheit und organisationsweite Sicherheitsanalysen in KMU“

[Zitierung:
Scholl, M. (2024). Schlussbericht des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“: Neue Wege für mehr Informationssicherheit in deutschen Klein- und mittelständischen Unternehmen. Wildau: TH Wildau.]

Zuwendungsempfänger	Förderkennzeichen
Technische Hochschule (TH) Wildau	01MS19002A

Autorin/Projektleitung: Prof. Dr. Margit Scholl

Laufzeit des Vorhabens: 01.10.2020 – 30.09.2023 / KNV 01.10.2023 – 31.03.2024

Erstellungsdatum: 27.03.2024

Inhaltsverzeichnis

1. Darstellung des Projektes

1.1 Aufgabe und Ziel des Projektes

Die Aufgaben entsprechend der Ziele sind dem nachfolgenden eingereichten Projektstrukturplan zu entnehmen. Lediglich die Zeitspanne wurde auf den Bewilligungszeitraum vom 01. Oktober 2020 bis 30. September 2023 verschoben. Die geplanten Ziele (Abb. 1) wurden erreicht.

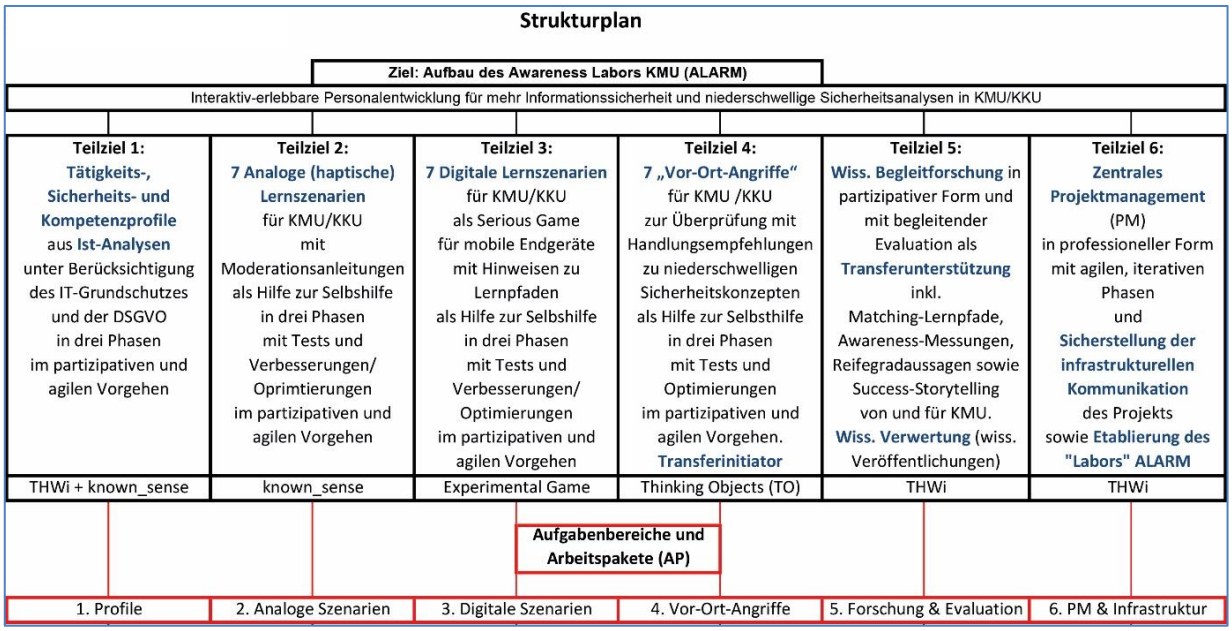


Abbildung 1 Strukturplan mit der Zielsetzung des Projekts „ALARM Informationssicherheit“

Strukturplan

THWi + known_sense	known_sense	Experimental Game	Thinking Objects (TO)	THWi	THWi
Aufgabenbereiche und Arbeitspakete (AP)					
1. Profile	2. Analoge Szenarien	3. Digitale Szenarien	4. Vor-Ort-Angriffe	5. Forschung & Evaluation	6. PM & Infrastruktur
AP 1.1 Ist-Analyse: Online Befragungen (THWi)	AP 2.1 Übertragung der Profile in verbindlich definierte Lernszenarien	AP 3.1 Konzeption des digitalen Serious Games	AP 4.1 Pilot-Unternehmen akquirieren und betreuen	AP 5.1 Angewandte Begleit-F&E, begleitende Evaluation, Qualifikationsbedarfe, IT-Grundschutz, wiss. Verw.	AP 6.1 Meetings und Abstimmung sowie Berichtswesen
AP 1.2 Ist-Analyse: Tiefenpsychologische Interviews (known_sense)	AP 2.2 Konzeption der analogen Lernszenarien	AP 3.2 Konzeption der digitalen Lernszenarien	AP 4.2 Konzeption der Angriffszenarien	AP 5.2 Sensibilisierung und Schulungen sowie Train-the-Trainer-Konzept	AP 6.2 Informationsveranstaltungen & Öffentlichkeitsarbeit
AP 1.3 2 Kreativworkshops, Auswertung, Austausch (known_sense)	AP 2.3 Agile Entwicklung Pilotversionen für analoge Lernszenarien	AP 3.3 Agile Entwicklung Pilotversionen für digitale Lernszenarien	AP 4.3 Agile Entwicklung Pilotversionen für Angriffe	AP 5.3 Agile Entwicklung Pilotversionen Awareness-Messungen KMU	AP 6.3 Qualitätsmanagement und Qualitätssicherung
AP 1.4 3 tiefenpsych. Studienreports (knonwn_sense)	AP 2.4 Testen der entwickelten analogen Szenarien	AP 3.4 Testen der entwickelten digitalen Szenarien	AP 4.4 Testen der entwickelten Vor-Ort-Angriffe	AP 5.4 Testen Awareness-Messungen; Entw. Reifegrad-Aussagen KMU	AP 6.4 Begleitendes Risikomanagement
AP 1.5 Interviewer-Briefings, Zwischen- und Endanalysen (known_sense)	AP 2.5 Transfer TO, THWi über Pilotunternehmen hinaus	AP 3.5 Transfer TO, THWi über Pilotunternehmen hinaus	AP 4.5 Transfer TO, THWi über Pilotunternehmen hinaus	AP 5.5 Unterstützung analoge, digitale LS, Angriffe. Eigener Transfer Awareness-Mess. & Reifegrad	AP 6.5 Change-Management & Ausschreibung/Beschaffung
AP 1.6 Report-Mapping quantitativer Forschungteil (known_sense)	AP 2.6 Transfer mit IHKs, DIZ	AP 3.6 Transfer mit IHKs, DIZ	AP 4.6 Transfer mit IHKs, DIZ	AP 5.6 Transferunterstützung sowie Success-Stories KMU/KKU	AP 6.6 Sicherung sowie Prüfung: Ziele und Strategie
AP 1.7 Tätigkeits-, Sicherheits-, Kompetenzprofile (THWi, known_sense)	AP 2.7 Transfer mit zentraler Transferstelle	AP 3.7 Transfer mit zentraler Transferstelle	AP 4.7 Transfer mit zentraler Transferstelle	AP 5.7 Transferunterstützung sowie Matching-Methode KMU/KKU	AP 6.7 Meilenstein-Trendanalyse (MTA) & Infrastruktur/Domain
AP 1.8 Erste Auswahl von Profilen für die betrieblichen Lernszenarien (known_sense, THWi)	AP 2.8 Finalisierung der Projektergebnisse analoge Lernszenarien inkl. Anleitungen & Produktion	AP 3.8 Finalisierung der Projektergebnisse digitale Lernszenarien (Serious Game) inkl. Hinweise für Lernpfade	AP 4.8 Finalisierung der Projektergebnisse Angriffe und niederschwellige Sicherheitskonzepte	AP 5.8 Finalisierung Matching, Awareness-Messungen, Reifegradaussagen, Success-Stories KMU, wiss. Verw.	AP 6.8 Finalisierung Gesamtergebnis, Projektdokumentation, Abschlussbericht und ALARM
known_sense: 60 PT THWi: 08 PMo	known_sense: 30 PT THWi: 07 PMo	Exp. Game: 114 PT THWi: 02 PMo	TO: 75 PT THWi: 03 PMo	THWi: 48,5 PMo	THWi: 26 PMo

PT = PersonenTage
PMo = Personenmonate

Abbildung 2 Strukturplan mit den geplanten und den Akteuren zugeordneten Aufgabenbereichen / Arbeitspaketen

Wie in der Projektdokumentation in Buchform bereits ausführlich beschrieben[1] und auch in etlichen weiteren Publikationen auf Deutsch und auf Englisch zum Projekt „ALARM Informationssicherheit“ in der Anlage 4.1 dokumentiert, war die Komplexität des praxisorientierten Projekts „ALARM Informationssicherheit“ von Beginn an klar, sollte es doch innerhalb von nur drei Jahren ein Gesamtszenario zur Sensibilisierung und Unterstützung der KMU für Informationssicherheit bis hin zu deren Selbsthilfe aufbauen (Scholl, 2024a). Die Einzelaufgaben der beteiligten Unterauftragnehmern und des Forschungsteam der TH Wildau sind den obigen Abbildungen (Abb. 1 und 2) zu entnehmen. Durch ein Insolvenzverfahren von Experimental Game wurde nach einer Neuausschreibung Gambebook Studio GmbH zuständig für die Aufgaben der digitalen Lernszenarien (Teilziel / Aufgabenbereich 3).

Das zugrunde liegende Forschungsdesign (Abb. 2) enthielt innerhalb einer zentralen Projektmanagementsteuerung vor allem neue Entwicklungen, die iterativ in drei Phasen, agil und partizipatorisch, ein innovatives Prozess-Szenario für Informationssicherheit mit analogen und digitalen erlebnisorientierten Szenarien sowie „Vor-Ort-Angriffen“ und weiteren Überprüfungen, wie z. B. Awareness-Messungen, Quiz und Tests beinhalteten (Scholl, 2024a). Der Anspruch des Gesamtszenarios war es, dass damit die dringend notwendige betriebliche Sensibilisierung von Führungskräften und Mitarbeitenden und die entsprechend gezielte Personalentwicklung in KMU gefördert wird, wie sie breitenwirksam bislang noch nicht vorhanden war (Scholl, 2024a). Dazu sollte IT-Sicherheit im Zusammenhang mit den zunehmend digitalen Arbeitsprozessen konkret (be-)greifbar gemacht und die Menschen gleichzeitig emotional berührt, aktiv und motivierend in die Entwicklung von Sensibilisierungsmaßnahmen einbezogen werden; eine nachhaltige und unternehmensweite Informationssicherheitskultur soll damit gestärkt und das Sicherheitsniveau in deutschen KMU erhöht werden (Scholl, 2024a).

Die angesetzten Personalmonate für das Forschungsteam der TH Wildau (s. Abb. 2) erwiesen sich u.a. infolge der erheblichen und neuen Herausforderungen der Corona-19-Pandemie seit 2020 als deutlich zu gering; durch Mittelumwidmungen wurde hier entgegengewirkt. Wie vorgesehen, stehen seit September 2023 alle wichtigen Materialien in erprobter digitaler und analoger Form zur Sensibilisierung von KMU-Mitarbeitenden auf der Projektwebseite

https://alarm.wildau.biz

kostenfrei für die interne, nicht-kommerzielle Nutzung zur Verfügung (Scholl, 2024a). Durch eine wirtschaftliche Projektführung konnte eine kostenneutrale Verlängerung (KNV) des Projekts mit einigen wenigen Personalstunden bis zum 31. März 2024 erreicht werden, so dass alle Ergebnisse in ihrer Qualität erneut überprüft und finalisiert werden konnten. Insbesondere die Serious Games mit Begleitmaterial wurden in neuen Veranstaltungen weiterhin und breitenwirksam deutschen Unternehmen und Netzwerkpartnern bekannt gemacht. Die Resonanz war durchweg sehr positiv. Die Projektdokumentation (Scholl, 2024a) als Buch und weitere Artikel auf Deutsch und auf Englisch sowie fünf Podcasts konnten in der KNV veröffentlicht werden.

1.2 Ausgangslage zu Beginn des Projektes

Aktuelle Studien zeigten, dass in den deutschen KMU inzwischen zwar technische Vorkehrungen zur Risikoreduzierung getroffen wurden, allerdings kein nennenswerter Anstieg in organisatorischen Maßnahmen für Informationssicherheit – inklusive Sensibilisierung und Schulung von Personal – zu verzeichnen war (bzw. ist) und zudem nur ein Drittel der befragten Unternehmen über einen Notfallplan verfügte. Waren dies allein schon bemerkenswerte Herausforderungen in der Zielsetzung des Projekts „ALARM Informationssicherheit“ so kamen neuen bislang nicht gekannten Schwierigkeiten durch die Corona-19-Pandemie hinzu, mit fast täglich sich veränderten Auflagen, die alle bisherigen Absprachen und Abläufe obsolet erscheinen ließen. Auch im Rückblick ist festzustellen, dass dies ein unfassbarer Mehraufwand aller Projektbeteiligten bedeutete (Scholl, 2024a).

[1] Margit Scholl (Hrsg.) (2024a). Neue Wege für mehr Informationssicherheit in KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit. Frankfurt/M.: Buchwelten Verlag, 234 Seiten.

Außerdem erwies sich sowohl die Rekrutierung der Pilot-KMU als auch danach die des KMU-Personals für die anonymisierten Interviews und deren Durchführung als äußerst schwierig (Scholl, 2024a). Darüber hinaus gestalteten sich die Vereinbarungen als sehr zeitaufwendig, da z. B. Termine teilweise (mehrfach) abgesagt wurden und verschoben werden mussten (Scholl, 2024a). Infolge der Rahmenbedingungen der Corona-Pandemie, Gespräche digital durchführen zu müssen, ergaben sich bei allen Projektbeteiligten zudem neue technisch-organisatorische Herausforderungen (Scholl, 2024a).

Es gab im Forschungsteam dieses Projekts viele bislang nicht erfahrene Personalveränderungen, sei es durch Krankheit, persönliche Weiterentwicklungswünsche, Familiengründungen, Geburten, Mutterschutz und Elternzeiten, und leider hatten wir auch den Tod eines Projektpartners zu beklagen. Diese Veränderungen gepaart mit der schwierigen allgemeinen Gesamtsituation führte zu kontinuierlich neu zu bewältigenden Herausforderungen, die sich auch in etlichen finanziellen Umwidmungsanträgen widerspiegelten. Umso mehr ist zu betonen, dass das Projekt „ALARM Informationssicherheit“ tatsächlich erfolgreich abgeschlossen wird. Dies wird mit der Projektdokumentation (Scholl, 2024a) auf Deutsch umfassend dargestellt und in weiteren Veröffentlichungen auch international verdeutlicht (Scholl, 2024b[2]; Scholl, 2024c[3]). Darüber hinaus wurde nach dem ersten Projektjahr bei einem Unterauftragnehmer ein Insolvenzverfahren durchgeführt und führte zur Neuausschreibung. Die Komplexität des Projekts „ALARM Informationssicherheit“ war daher unter unterschiedlichen Aspekten enorm.

1.3 Struktur des Projektes

Die inhaltliche und organisatorische Aufgabenverteilung ist ebenfalls den obigen Abbildungen (Abb. 1 und 2) mit den sechs Teilzielen und entsprechenden Aufgabenbereiche sowie Arbeitspaketen zu entnehmen.

1.3.1 Partner

Für die tiefenpsychologischen Interviews mit den vier Pilotunternehmen des Projekts war der Unterauftragnehmer known_sense zuständig (Teilziel / Aufgabenbereich 1). Es resultierten die geplanten drei Studien (s. Veröffentlichungsliste in Anlage 4.1). Die erste Studie bildete den Ausgangspunkt für die Entwicklung aller Materialien. Die Firma known_sense war auch für die Entwicklung der sieben analogen Serious Games verantwortlich (Teilziel / Aufgabenbereich 2). Diese Entwicklung wurde in kontinuierlicher Abstimmung mit dem Forschungsteam der TH Wildau und iterativ mit Erprobungen in der Praxis durchgeführt. Genaueres siehe die Projektdokumentation in Buchform (Scholl, 2024a).

Für die Entwicklung der sieben digitalen Serious Games in enger Absprache und Betreuung mit dem Forschungsteam der TH Wildau sowie in Erprobung mit den Pilotunternehmen wurde der Unterauftragnehmer Gamebook Studio GmbH verantwortlich (Teilziel / Aufgabenbereich 3). Details siehe die Projektdokumentation in Buchform (Scholl, 2024a) und die Veröffentlichungsliste in Anlage 4.1.

Die „Vor-Ort-Angriffe“ bei den beteiligten KMU wurden vom Unterauftragnehmer Thinking Objects GmbH konzipiert und in Abstimmung mit dem Forschungsteam der TH Wildau durchgeführt (Teilziel / Aufgabenbereich 4). Daraus wurden wie geplant sieben niederschwellige Sicherheitskonzepte für KMU und entsprechende Informationsblätter entwickelt, die in Scholl (2024a und 2024c) ausführlich beschrieben werden.

Die Firma sudile GbR unterstützte als Unterauftragnehmer insbesondere das Teilziel / Auf-

[2] Scholl, M. (2024b). Summary of the project documentation “Awareness Lab SME (ALARM) Information Security” doi:10.13140/RG.2.2.20336.64002/1

[3] Scholl, M. (2024c). Résumé of the Gamified Increase in Security Awareness in German Small and Medium-Sized Businesses after Three Years’ Practice of “ALARM Information Security”, doi:10.13140/RG.2.2.13519.29600

gabenbereich 5 des Projekts (Abb. 1 und 2) und mit Dr. Brüggemann vor allem bei dem Versuch, ein mathematisch fundiertes Matching abzuleiten, zu dessen Problematik zwei beachtete Artikel auf Englisch veröffentlicht wurden (s. Veröffentlichungsliste in Anlage 4.1). Aus diesen Überlegungen resultierte gemeinsam mit dem Forschungsteam der TH Wildau ein vorher im Projektantrag nicht geplanter Selbsttest für Individuen (SeSec) zur Einschätzung des eigenen Informationssicherheitsbewusstseins, der ebenfalls auf der Projektwebseite frei zur Verfügung steht.

Das Forschungsteam der TH Wildau war in allen Arbeitspaketen sehr aktiv beteiligt und hat weitere digitale Ergänzungen entwickelt, die auf der Projektwebseite zur Verfügung stehen. Das Forschungsteam führte im Aufgabenbereich 1 (Profile) parallel zu den tiefenpsychologischen Interviews durch known_sense Online-Umfragen durch, die als Report 1 veröffentlicht wurden. Report 2 wurde von dem verantwortlichen Mitarbeiter bis Vertragsende am 30. September 2023 nicht final zum Druck fertig gestellt und daher bislang nicht veröffentlicht – ein kurzer Abriss wird in Scholl (2024a) gegeben[4]. Das von dem verantwortlichen Mitarbeiter entwickelte Modell zur Sicherheitskultur in KMU ist von ihm in Schuktomow u.a. (2023)[5] dargestellt. Insofern kann durch die Veröffentlichung Schuktomow u.a. (2023) auch Report 2 als erfüllt angesehen werden. Report 3 dient als Abschlussevaluation (s. Veröffentlichungsliste in Anlage 4.1 und Anlage 4.2.2).

Neben dem Projektmanagement und einer aktiven Beteiligung an allen Arbeitspaketen, den Reports im Teilziel / Aufgabenbereich 1 und der eigenen Durchführung vielfältiger Sensibilisierungsmaßnahmen mit einer aktiven Öffentlichkeitsarbeit zu den Projektergebnissen lag der geplante Schwerpunkt des Teams der TH Wildau im Teilziel / Aufgabenbereich 5 (Forschung mit Veröffentlichungen & Evaluation) als auch im Teilziel / Aufgabenbereich 6 (zentral & agiles Projektmanagement, Qualitätssicherung, Infrastruktur etc.). Aufgrund der durchweg positiven Resonanz der Sensibilisierungsmaßnahmen und öffentlichen Darstellungen des Projekts „ALARM Informationssicherheit“ durch das Forschungsteam der TH Wildau kam es zudem auf vielfältigem Wunsch zu zwei Moderatorenausbildungen von Mitarbeitenden aus KMU und Netzwerkpartnern, die im ursprünglichen Projektantrag nicht vorgesehen war. Der Mehraufwand für das Team der TH Wildau im Projekt „ALARM Informationssicherheit“ erhöhte sich während der Projektdurchführung daher aus vielfältigen Gründen in einem Maß, das bei Antragsstellung nicht vorhersehbar war und führte zu etlichen Umwidmungen von Mitteln vor allem der Projektpauschale und Dienstreisen zwecks Aufstockung von Projektpersonal.

1.3.2 Arbeitsplanung

Die Arbeitsplanung verlief wie im Projektantrag ausgeführt und vereinbart. Genaueres ist der Projektdokumentation in Buchform (Scholl, 2024a) zu entnehmen. Allerdings waren die Herausforderungen auch für das Projektmanagement in diesem komplexen Projekt unter Corona-Bedingungen enorm. Es muss daher festgehalten werden, dass ohne das äußerst engagierte Forschungsteam der TH Wildau, das nur durch befristete Teilzeit-Projektverträge finanziert wurde, die hochwertigen Ergebnisse des Projekts „ALARM Informationssicherheit“ nicht möglich gewesen wären. Mit eigenen hohen Ansprüchen, großem Enthusiasmus und einem gewollt nahen Praxisbezug war dieses komplexe Projekt auch für das lösungsorientierte Team der TH Wildau in den unterschiedlichen Konstellationen stressig und die Bildung einer persönlichen Resilienz war erforderlich.

[4] von Tippelskirch, H., Scholl, M. & Prott, F. (2024). Umfragen und Reports. Kapitel 2.2.2 "Report 2: Informationssicherheitskultur in KMU". In: Scholl, M. (2024a), S. 43f.

[5] Schuktomow, R., von Tippelskirch, H., & Scholl, M. (2023). Informationssicherheit in den Arbeitsalltag nachhaltig integrieren: Informationssicherheitskultur verstehen, mit Serious Games sensibilisieren und das Informationssicherheitsbewusstsein der Mitarbeitenden erhöhen. (C. Czarnecki, A. Lübbe, V. G. Meister, C. Müller, M. Steglich, & M. Walther), *Angewandte Forschung in der Wirtschaftsinformatik 2023 : Tagungsband zur 36. AKWI-Jahrestagung vom 11.09.2023 bis 13.09.2023 ausgerichtet von der Technischen Hochschule Wildau*. Wildau: Technische Hochschule Wildau. doi:10.15771/1794 (**Report 2**)

1.4 Zusammenarbeit mit …

1.4.1 Unterauftragnehmern

Die Zusammenarbeit mit den bereits genannten Unterauftragnehmern verlief professionell gut und war notwendig, da sie als ausgewiesene Experten in spezifischen Teilbereichen des Projekts „ALARM Informationssicherheit“ zur Ergebnissicherung beitrugen. Die Probleme infolge des Insolvenzverfahrens eines Unterauftragnehmers konnten im Projektverlauf behoben werden. Spezifische Erkenntnisse aus den einzelnen Aufgabenbereichen des Projekts ist der umfassenden Projektdokumentation in Buchform (Scholl, 2024a) zu entnehmen und werden hier im Kapitel 2 skizziert.

1.4.2 Assoziierten Partnern

Aktive assoziierte Projektpartner waren drei IHK aus Brandenburg: IHK Ostbrandenburg, IHK Potsdam und IHK Cottbus. Es wurde ein nachhaltiger intensiver Austausch in allen Phasen des Projektes gepflegt. Ein Mitarbeiter der IHK Ostbrandenburg lies sich zudem als Moderator ausbilden und nutzt die erzielten finalen Projektergebnisse aktiv im Rahmen seiner KMU-Kontakte. Darüber hinaus wurde von der IHK auch der Kontakt zu der Handwerkskammer (HWK) Potsdam hergestellt. Gemeinsam mit der HWK Potsdam wurden während der kostenneutralen Verlängerung (KNV) des Projekts bis März 2024 zwei Events zur Bekanntmachung der Projektergebnisse für Handwerksbetriebe erfolgreich durchgeführt (siehe auch Kapitel 2.2.1 sowie Abbildungen 14 und 15). Ein IHK-Evaluationsbericht mit Ausblick zum praktischen Einsatz des „Awareness-Koffer“ mit den analogen Serious Games im KNV-Zeitraum bis Februar 2024 ist im Kapitel 4.2.5 zu finden.

1.4.2 Netzwerk Mittelstand-Digital

Das Forschungsteam der TH Wildau hat von Beginn an eine sehr aktive Öffentlichkeitsarbeit geleistet und an den Terminen sowohl der ehemaligen Transferstelle „TiSim“ bis September 2023 als auch der neuen zentralen Transferstelle der Mittelstandinitiative „CYBERsicher“ bis März 2024 teilgenommen. Die weiteren offiziellen Vernetzungen in Folge des Projekts „ALARM Informationssicherheit“ sind der Projektwebseite unter der Rubrik „Vernetzung“ zu entnehmen.

2. Ergebnisse / Zielerreichung

2.1 Ist-Soll Abgleich quantifizierbarer Ergebnisse

Das Projekt „ALARM Informationssicherheit“ hat seine im Projektantrag formulierten Ziele erreicht (Abb. 1) und trägt durch die qualitativ hochwertigen und praxiserprobten Endprodukte entsprechend der Aufgabenbereiche (Abb. 2) zur Erhöhung der Informationssicherheit in KMU bei:

- Sieben analoge Serious Games inklusive vielfältiger Anleitungen (s. Abb. 3);
- sieben digitale Serious Games mit integriertem Feedback für die spielend Lernenden (s. Abb. 4);
- ein Selbsttest und digitale Ergänzungen (s. Abb. 4 und 3);
- sieben themenorientierte Informationsblätter und niederschwellige Sicherheitskonzepte für KMU (s. Abb. 5);
- aktive Vernetzung des Projekts mit anderen Mittelstandsaktivitäten;
- Materialen wie Flyer, Broschüren, Poster für eine aktive Öffentlichkeitsarbeit;
- Bekanntmachung des Projekts durch Veranstaltungen und in Presse, Rundfunk und Fernsehen;
- umfassende Verwertung durch wissenschaftliche Artikel auf Deutsch und auf Englisch, die Studien und Reports des Projekts auf Deutsch sowie Podcasts auf Englisch auch für eine internationale Verwertung (s. Abb. 6 - 10) – auch der IHK-Evaluationsbericht (Kapitel 4.2.5)

verdeutlicht den Wunsch deutscher KMU mit englischsprachigen Mitarbeitenden nach Materialien auf Englisch;
- ein Video auf Deutsch mit Reflexionen von beteiligten Pilotunternehmen und Nutzenden enthält eine zusammenfassende Veranschaulichung und Evaluation zum Projekt (Abb. 11).

Für die heterogene deutsche KMU-Landschaft gibt es bei den im Projekt „ALARM Informationssicherheit“ entwickelten analogen Serious Games (Abb. 3) einen großen Vorteil (Pokoyski & Hauke 2022): Ihr auf Differenzierung ausgelegter modularer Ansatz mit der Möglichkeit individueller Adaptierbarkeit unterstützt die KMU, diese große Bandbreite für sich selbst in den Serious Games durch eigene praktische Beispiele zu ergänzen und damit praxisorientiert und spezifiziert auf ihre eigenen Bedürfnisse anzupassen.[6] Insofern hat das Projekt „ALARM Informationssicherheit“ auch seinen Ansatz „Hilfe zur Selbsthilfe“ für KMU erreicht.

Abbildung 3 Zielerreichung (Aufgabenbereich 2) durch sieben analoge Serious Games jeweils mit Moderationsanleitung, Konstruktionsanleitung, Handout und Druckvorlagen zum Download. Darüber hinaus ein Infoblatt zum Storykonzept der analogen Lernszenarien und eine digitale Ergänzung zum Infoklassen-Roulette-Spiel. Quelle: https://alarm.wildau.biz/

Auch die Befragungsergebnisse und Gesamtevaluation der digitalen Serious Games (Abb. 4) fiel insgesamt sehr positiv aus[7]. Die Charaktere der digitalen Serious Games werden über alle Spiele hinweg als realitätsnah beurteilt und die abschließende Auswertung in den digitalen Spielen wird von den Testusern als nachvollziehbar empfunden. Allerdings motiviert das gegebene Feedback eher weniger dazu, über die getroffenen Entscheidungen nachhaltig nachzudenken, weshalb wir dringend eine Nachbesprechung der Thematik empfehlen, wenn nur digitale Spiele zur Sensibilisierung eingesetzt werden.

Der "Security Self Check – Selbsttest (SeSeC)"[8] (Abb. 4) ist eine niederschwellige Sensibilisierungsmaßnahme, die Daten generiert, den Wissenstand der Teilnehmenden ermittelt, den Vergleich mit anderen Selbsttestusern erlaubt und mit einer Sofortauswertung den Wissenstand der Teilnehmenden erweitert bzw. auffrischt. Dies wurde notwendig, weil die Festlegung von Tätigkeitsfeldern zeitintensiver als vorgesehen war und vor allem die darauf aufbauenden

[6] Pokoyski, D. & Haucke, A. (2022). Enabling vs. Entmündigung. Scholl, M. (Ed.) (2022b), Wildau: TH Wildau. Download: https://alarm.wildau.biz/static/c0e4d00beefe1dc5fac9b50b6087265f/studie-2-master-final.pdf (**Studie 2**)
[7] Scholl, M., Prott, F. & Küchler, U. (2024). Digitale Serious Games als Sensibilisierungsmethode für mehr Informationssicherheitsbewusstsein. In: Scholl, M. (2024a), S. 57ff.
[8] Koppatz, P. (2024). Security Self Check (SeSeC) – Selbsttest zur individuellen Wissenstandsermittlung. In: Scholl, M. (2024a), S. 89ff.

Awareness-Messungen erst zu einem späteren Zeitpunkt und nur rudimentär auswertbare Ergebnisse bringen konnten. So begann mit dem Selbsttest frühzeitig eine zusätzliche, im Projektantrag nicht vorgesehende, parallele Entwicklung, um grundsätzliche Fragen für automatisierte Empfehlungen geben zu können. Damit bilden die gesammelten Daten die Basis für wissenschaftliche Betrachtungen (Koppatz, 2024). Zentrales Ziel war die Ermittlung von Indikatoren und den daraus berechneten Lernpfaden bzw. Empfehlungen für zielgenaue Sensibilisierungsmaßnahmen, die sich aus den durch den Selbsttest erkennbaren Wissenslücken ergeben.

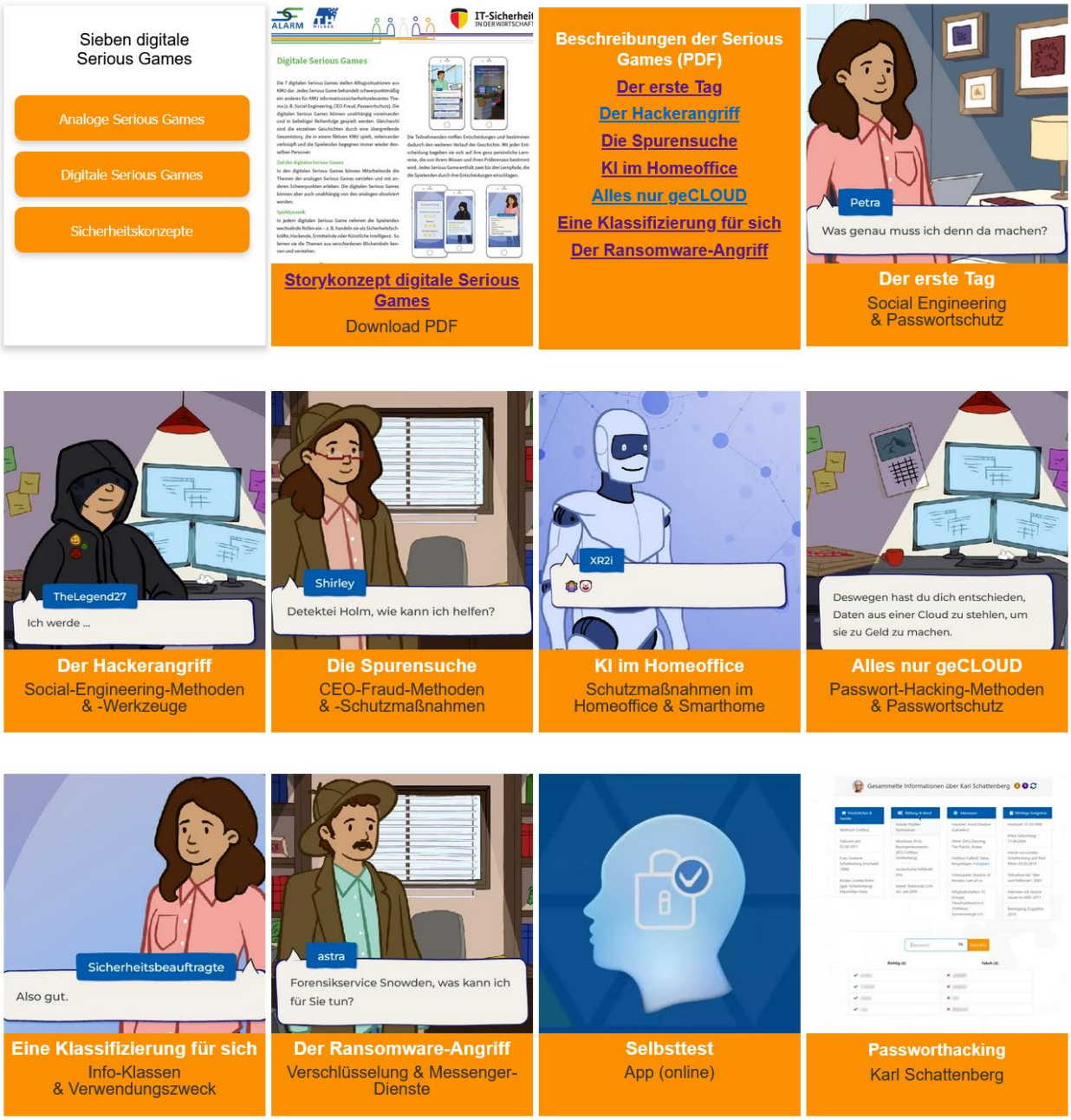


Abbildung 4 Zielerreichung (Aufgabenbereich 3) durch sieben digitale Serious Games zur Informationssicherheit und ein Infoblatt zum Storykonzept sowie zwei digitale Ergänzungen (Selbsttest und Passworthacking). Die digitalen Lernszenarien können direkt auf der Projektwebseite gespielt werden; Spielende erhalten am Ende ein direktes Feedback. Quelle: https://alarm.wildau.biz/

Das digitale Spiel „Passworthacking“ für KMU (Abb. 4) wurde ebenfalls zusätzlich vom Forschungsteam der TH Wildau entwickelt und basiert auf der Idee eines schon länger an der TH Wildau eingesetzten Lernszenarios aus der „Secrurity Arena“ von known_sense. Seine Neuentwicklung wurde vorgenommen, da sich die Entwicklung der digitalen Lernszenarien infolge des Insolvenzverfahrens des ursprünglichen Unterauftragnehmers, Experimental Game, dramatisch

verzögerte. Das Zeit- und Inhaltsdefizit wurde von dem Nachfolger, Gamebook Studio GmbH, souverän behoben.

Der Bedarf und die Notwendigkeit, „Vor-Ort-Angriffe“ innerhalb von Awareness-Programmen einzusetzen, belegen unsere Ergebnisse und Erfahrungen innerhalb des Forschungsprojekts. Diese Szenarien können auf der einen Seite positive Belege für die langjährige und stetige Investition in die Sicherheitskultur in Unternehmen liefern und zugleich im Gegensatz dazu bei Unternehmen, die noch am Anfang einer Sicherheitskulturentwicklung stehen, wichtige Impulse und Hinweise liefern, welche relevanten Security-Bausteine verfolgt werden sollten.[9] Der Einsatz von „Vor-Ort-Angriffen“ ermöglicht es sowohl die technische Perspektive von Sicherheitsfachkräften innerhalb der Unternehmen mit einzubeziehen als auch die Perspektive der Endanwenderinnen und Endanwender zu berücksichtigen (Vogt, 2024).

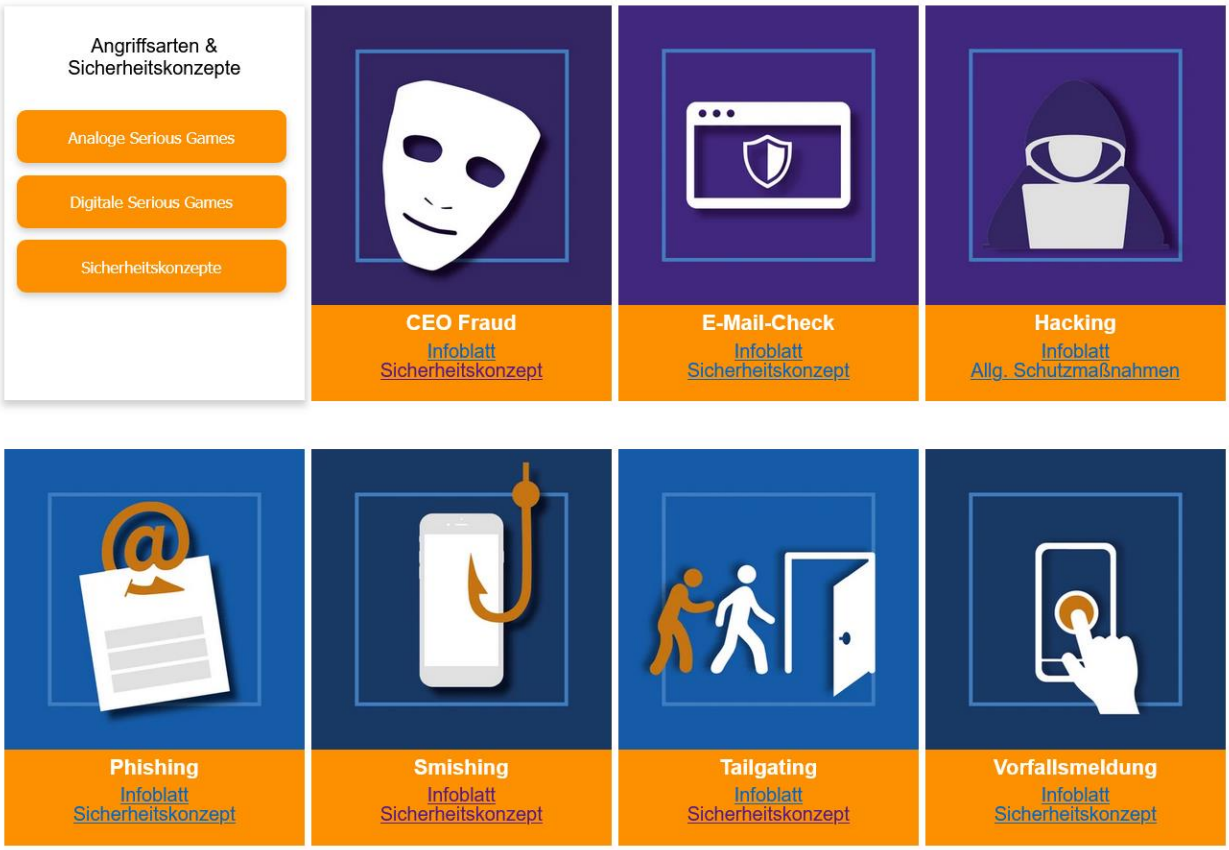


Abbildung 5 Zielerreichung (Aufgabenbereich 4) durch sieben niederschwellige Sicherheitskonzepte und Informationsblätter für KMU, die zum Download bereitstehen; entwickelt nach den durchgeführten sieben „Vor-Ort-Angriffen“ bei Pilotunternehmen und KMU-Kunden. Quelle: https://alarm.wildau.biz/

Aus diesem Teilziel / Aufgabenbereich 4 des Projekts „ALARM Informationssicherheit“ (Abb. 1 und 2) lassen sich wichtige Erkenntnisse ableiten, die für die weitere Entwicklung von Sensibilisierungsprogrammen relevant sind: Menschen profitieren von solchen erfahrungsbasierten Lernformaten. Diese sollten sich aber nicht ausschließlich auf Phishing-Simulationen beziehen, wie es viele Anbieter von Awareness-Maßnahmen auf dem Markt suggerieren (Vogt, 2024).

Cyberangriffe gelingen auf unterschiedlichen Wegen und als IT-Security-Expertinnen und -Experten ist es unser Auftrag, die unterschiedlichen Einfallstore zu benennen und umfassende Handlungsanweisungen sowohl an Mitarbeitende als auch an die Geschäftsführung und IT-Verantwortliche rauszugeben; ein umfassendes Risikoverständnis bei Mitarbeitenden lässt sich unserer Erfahrung nach am besten durch thematisch und methodisch abwechslungsreiche

[9] Vogt, M. (2024). Vor-Ort-Angriffe, niederschwellige Sicherheitskonzepte und Handlungsempfehlungen. In: Scholl (2024a), S. 77ff.

Informationssicherheit wurden Handlungsempfehlungen / Infoblätter und niederschwellige Sicherheitskonzepte für KMU (Abb. 5) erstellt.

In den weiteren Abbildungen (Abb. 6 – 11) werden die zusätzlichen Materialien für eine aktive Öffentlichkeitsarbeit im Projekt „ALARM Informationssicherheit“ dargestellt, die auf der Projektwebseite – über das Projektende hinaus auch für weitere Jahre – zur Verfügung stehen.

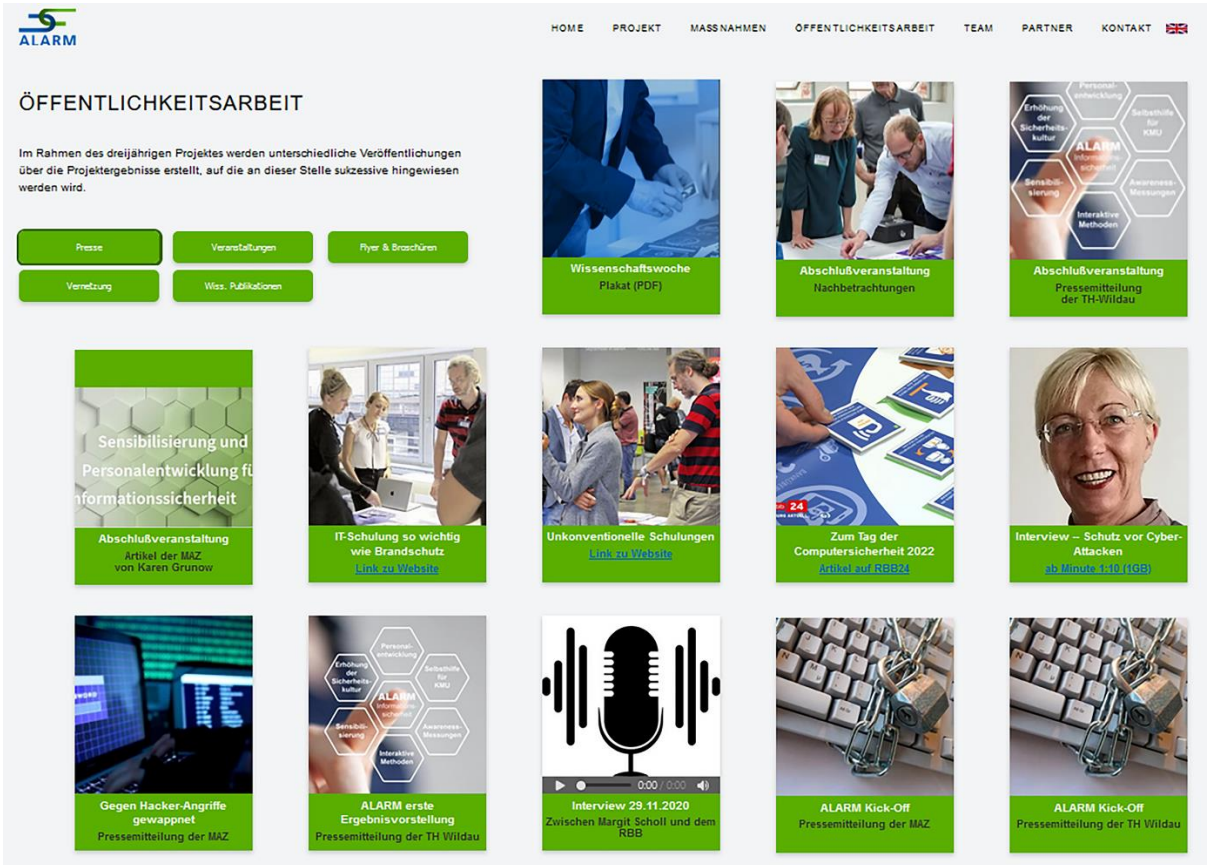


Abbildung 6 Zielerreichung (Arbeitsbereiche 5 und 6) durch aktive Pressearbeit. Quelle: https://alarm.wildau.biz/, Stand: 16.03.2024

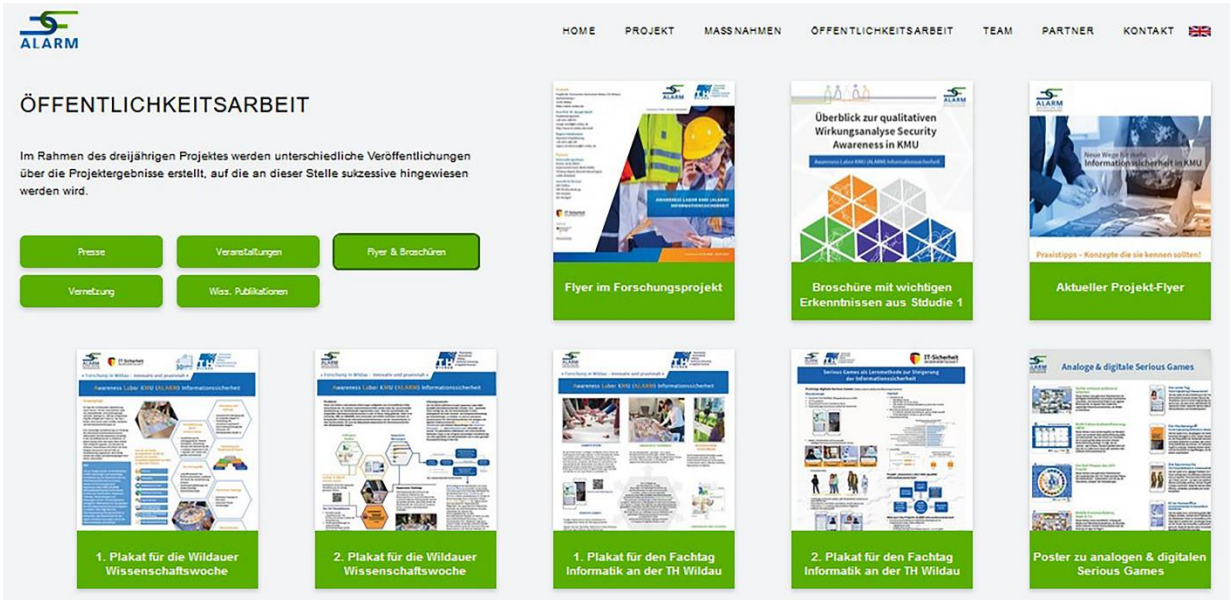


Abbildung 7 Zielerreichung (Aufgabenbereiche 5 und 6) durch aktive Öffentlichkeitsarbeit (Flyer & Broschüren). Quelle: https://alarm.wildau.biz/, Stand: 16.03.2024.

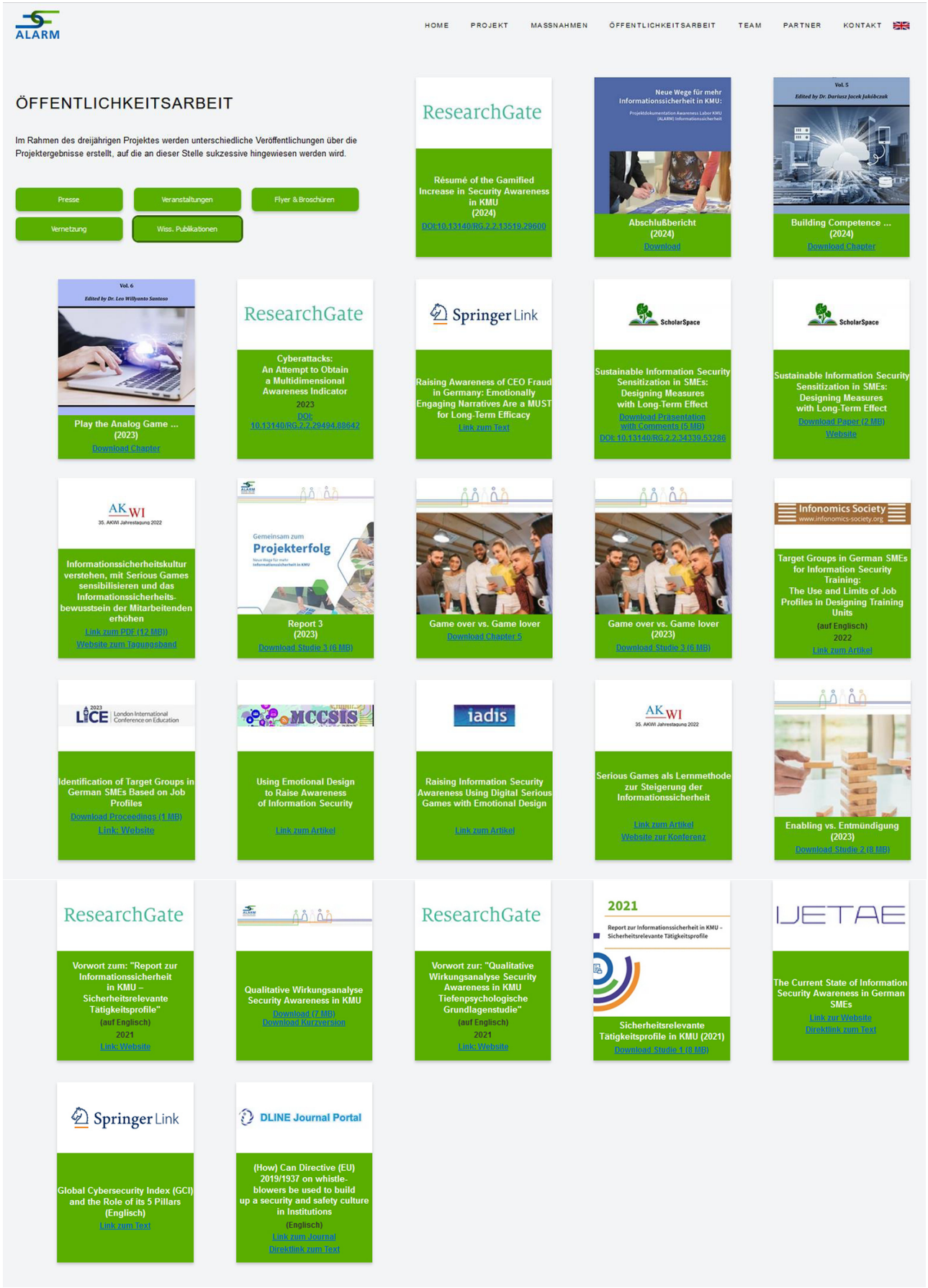


Abbildung 8 Zielerreichung (Arbeitsbereich 1 und Arbeitsbereich 5) durch Studien, Reports und weiteren wissenschaftlichen Veröffentlichungen. Quelle: https://alarm.wildau.biz/, Stand: 27.03.2024.

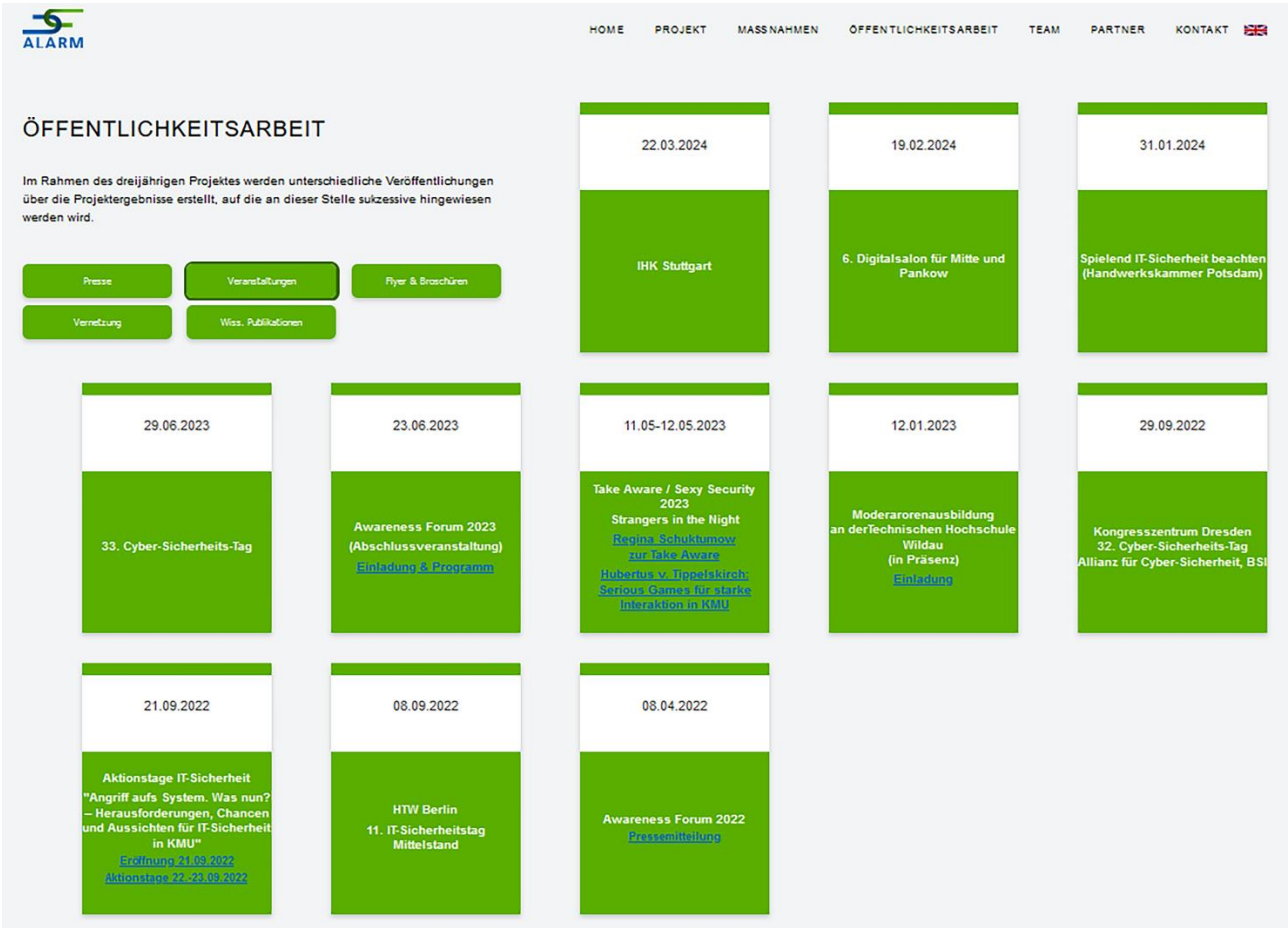


Abbildung 9 Zielerreichung (Aufgabenbereiche 5 und 6) durch Initiierung und Durchführung von sowie Beteiligung an Veranstaltungen. Die Projektwebseite zeigt hier nur Beispiele. Quelle: https://alarm.wildau.biz/, Stand: 16.03.2024.

Abbildung 10 Zielerreichung KMU-Sensibilisierung zum Gesamtprojekt: für deutsche KMU mit englischsprachigen Mitarbeitenden und insgesamt auch für ein internationales Publikum anhand von fünf Podcasts, produziert von ResearchPod im März 2024. Quelle: https://alarm.wildau.biz/, unter der Rubrik „Presse". Stand: 16.03.2024.

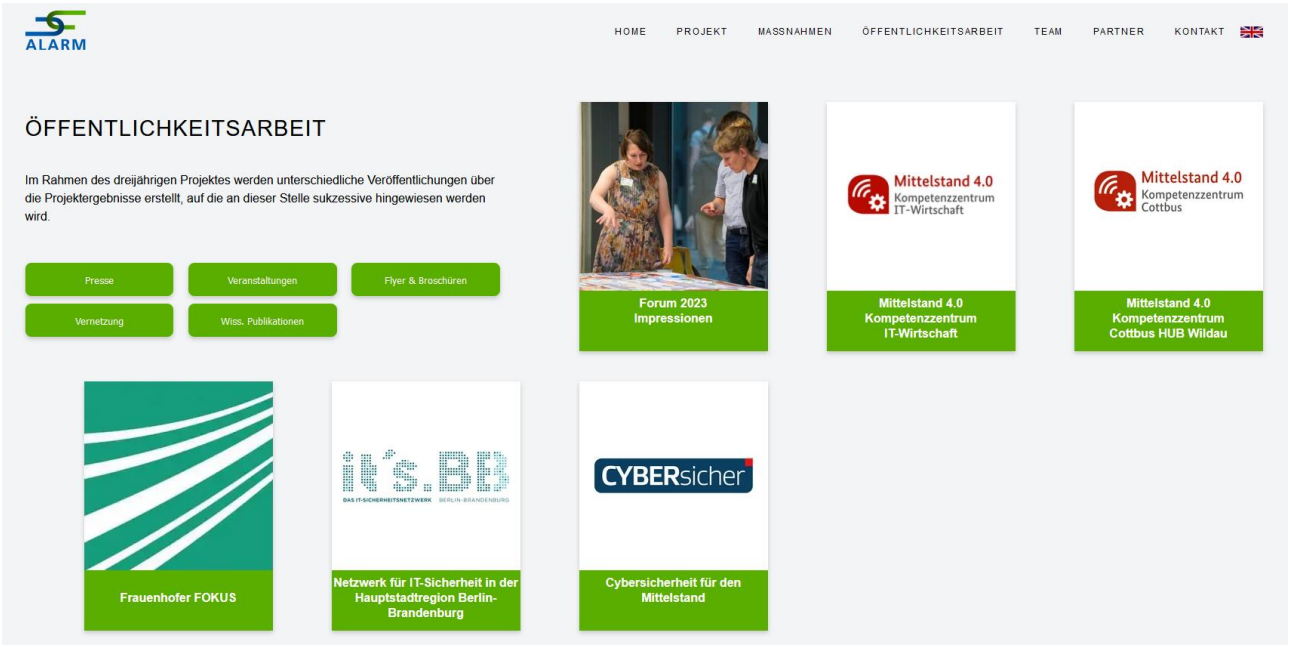


Abbildung 11 Zielerreichung KMU-Sensibilisierung des Gesamtprojekts international anhand Vernetzungsaktivitäten bis März 2024. Quelle: https://alarm.wildau.biz/, Stand: 18.03.2024.

Abbildung 12 Zielerreichung des Gesamtprojekts „Awareness Labor KMU (ALARM) Informationssicherheit“ dargestellt anhand eines Videos. Quelle: https://alarm.wildau.biz/, Stand: 30.09.2023.

2.2 Darstellung inhaltlicher Ergebnisse

2.2.1 Zentrale Projektleistungen

Alle erbrachten Leistungen inklusive Qualitätssicherungsmaßnahmen verdeutlichen die Notwendigkeit einer ganzheitlichen Betrachtungsweise von Informationssicherheit und einer integrativen Verzahnung von verschiedenen Methoden zur Sensibilisierung von KMU-Mitarbeitenden. Insgesamt sind folgende Leistungen zu relevanten Themen der Informationssicherheit erarbeitet worden:

3 Wissenschaftliche Studien auf Deutsch zu Informationssicherheit in KMU und Lernszenarien aus tiefenpsychologischen Interviews (Abb. 7)

2 Wissenschaftliche Reports auf Deutsch, zum einen aus der KMU-Onlineumfrage und zum andern aus der Evaluationsbefragung (Abb. 7)

1 Übersicht Storykonzept der analogen Lernszenarien für KMU auf Deutsch (Abb. 3)

7 Analoge Serious Games für KMU auf Deutsch, jeweils mit Handout, Moderationsanleitung inklusive „Goldene Regeln“, Konstruktionsanleitung und Druckvorlagen (Abb. 3):

- LS 1: Sicher Zuhause Arbeiten und Wohnen (Homeoffice)
- LS 2: Passwortschutz und Multi-Faktor-Authentifizierung
- LS 3: Die 5 Phasen des CEO-Frauds
- LS 4: Mobile Kommunikation, Apps & Co.
- LS 5: Cyber Pairs (Social-Engineering-Methoden)
- LS 6: Daten- und Informationsschutz
- LS 7: Informationsklassen-Roulette

1 Übersicht Storykonzept der digitalen Lernszenarien für KMU auf Deutsch (Abb. 4)

7 Beschreibungen der digitalen Serious Games für KMU auf Deutsch (Abb. 4)

7 Digitale Serious Games für KMU auf Deutsch, jeweils mit Feedback für die Spielenden (Abb. 4):

- LS 1: Der erste Tag
- LS 2: Der Hackerangriff: Social-Engineering-Methoden & -Werkzeuge
- LS 3: Die Spurensuche: CEO-Fraud-Methoden & -Schutzmaßnahmen
- LS 4: KI im Homeoffice: Schutzmaßnahmen im Homeoffice & Smarthome
- LS 5: Alles nur geCLOUD: Passwort-Hacking-Methoden & Passwortschutz
- LS 6: Eine Klassifizierung für sich: Informationsklassifizierung & Verwendungszweck
- LS 7: Der Ransomware-Angriff: Verschlüsselung & Messenger-Dienste.

1 Digitaler Security Selbsttest (SeSec) auf Deutsch für KMU-Mitarbeitende (Abb. 4)

1 Digitales Passwort-Hacking-Spiel auf Deutsch: Social-Media-Profil knacken für KMU (Abb. 4)

7 Infoblätter für KMU aus „Vor-Ort-Angriffen“ zu den Themen CEO Fraud, E-Mail-Check, Hacking, Phishing, Smishing, Tailgaiting und Vorfallsmeldung auf Deutsch als Überblick und Ergänzung zu den niederschwelligen Sicherheitskonzepten (Abb. 5)

7 Niederschwellige Sicherheitskonzepte auf Deutsch für KMU aus „Vor-Ort-Angriffen“ (Abb. 5):

- LS 1: Sicherheitskonzept CEO Fraud
- LS 2: Sicherheitskonzept E-Mail-Check
- LS 3: Sicherheitskonzept Hacking
- LS 4: Sicherheitskonzept Phishing
- LS 5: Sicherheitskonzept Smishing
- LS 6: Sicherheitskonzept Tailgating
- LS 7: Sicherheitskonzept Vorfallsmeldung.

35 Veranstaltungen, Workshops, Demonstrationen bis September 2023 (s. Beispiele in Abb. 9)

2 Moderatorenschulungen (s. Abb. 9)

1 Video auf Deutsch über das Projekt mit Evaluationsaspekten (Abb. 12)

1 Projektdokumentation in Buchform (Erstellung und Finalisierung während der KNV; veröffentlicht im März 2024) (Abb. 19)

7	Events von Januar 2024 bis zum 22. März 2024 in Wildau, Berlin, Potsdam, Caputh, Stuttgart (s. Beispiele in Abb. 13 bis 16)
5	Podcasts auf Englisch für die internationale Bekanntmachung der Projektergebnisse (Abb. 10)
13	Presseartikel (Abb. 6)
8	Flyer/Broschüren/Poster (s. Abb. 17 und Abb. 18)
6	Spezifische Vernetzungsinitiativen (s. Projektwebseite und Abb. 11)
28	Zusätzliche Artikel/Veröffentlichungen auf Deutsch und Englisch zu allen Teilzielen bzw. Aufgabenbereichen des Projekts als wissenschaftliche Verwertung (s. Abb. 7).

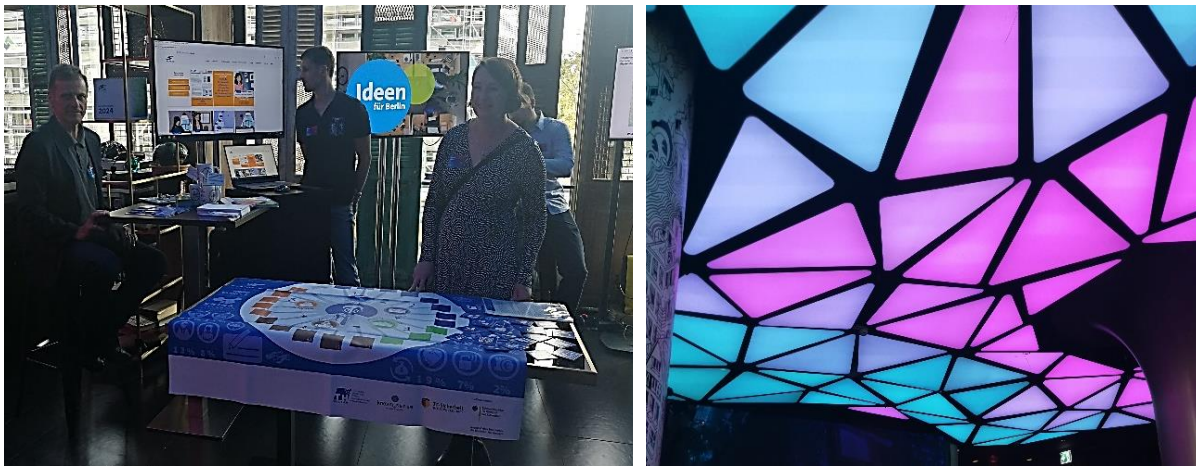


Abbildung 13 Zielerfüllung KNV: Beispiel Standsituation des Projekts „ALARM Informationssicherheit“ beim Event der Digitalagentur Berlin am 11. Oktober 2023.

Abbildung 14 Zielerfüllung KNV: Beispiel Standsituation des Projekts „ALARM Informationssicherheit“ beim Event der Handwerkskammer in Potsdam am 7. Dezember 2023.

Abbildung 15 Zielerfüllung KNV: Beispiel Spielsituation des Projekts „ALARM Informationssicherheit“ beim Event der Handwerkskammer in Caputh am 31. Januar 2024.

Abbildung 16 Zielerfüllung KNV: Beispiel Spielsituation des Projekts „ALARM Informationssicherheit“ beim Event „Digitalsalon“ der Digitalagentur Berlin am 19. Februar 2024 in Clubatmosphäre.

Abbildung 17 Zielerfüllung KNV: Beispiel Spielsituation des Projekts „ALARM Informationssicherheit“ beim Event „Cyber-Angreifende hacken Mitarbeitende und Führungskräfte - was sollten KMU tun?“ der IHK Stuttgart am 22. März 2024. Bild von TO.

Abb. 17 Fortsetzung der Impression von ‚Stuttgart 22.03.2024


Abb. 17 Fortsetzung der Impression von ‚Stuttgart 22.03.2024, Serious Game „CEO Fraud“.



Abb. 17 Fortsetzung der Impression von ‚Stuttgart 22.03.2024, Serious Game „Cyber Pairs“.

Abb. 17 Fortsetzung der Impression von ‚Stuttgart 22.03.2024, Serious Game „Zwei-Faktoren-Authentifizierung“

Abbildung 18 Projekte vielfältig, für KMU, für Studierende, aber auch für Schulen… Quelle: https://wildau.biz

Abbildung 19 Zielerfüllung KNV: Neuer Flyer zu den Ergebnissen des Projekts „ALARM Informationssicherheit“.

ALARM
Awareness Labor KMU Informationssicherheit

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

» Forschung in Wildau – innovativ und praxisnah «

Neue Wege für mehr **Informationssicherheit** in KMU

Reden Sie über das Thema Sicherheit bevor der Notfall eintritt. Unsere analogen Spiele unterstützen Sie dabei.

Einsatzmöglichkeiten der einzelnen Serious Games

- Teil eines ganzheitlichen Awareness-Konzepts
- Kombination mit anderen Serious Games dieses Formats als Awareness-Training (Stationenlernen-Methode)
- Als Einstieg oder Auflockerung einer Schulung zum Thema des Serious Games (z. B. CEO Fraud)
- Zeitrahmen: 15–45 Minuten (je nach gewünschter Intensität)
  Durchführung: 1 moderierende Person & 6–8 Teilnehmende

Sicher zuhause wohnen & arbeiten
Dieses Serious Game gibt einen Überblick über die wichtigsten betrieblichen und privaten Informationssicherheits- und Datenschutz-risiken in der eigenen Wohnung bzw. im eigenen Haus sowie über zugehörige Präventionsmaßnahmen, um Risiken zu minimieren.

Multi-Faktor-Authentifizierung (MFA)
Dieses Serious Game vereint Aspekte von Passwortschutz und der Multi-Faktor-Authentifizierung (MFA) und demonstriert, dass der Schutz von Informationen in einem großen Maße von einer sicheren Authentifizierung abhängt. Es zeigt, wie ein „starkes", weil sicheres, Passwort gebildet wird und dass ein (1!) Faktor zum Schutz sehr sensibler Informationen nicht ausreichend ist.

Die fünf Phasen des CEO Frauds
Hier wird ein Überblick über den Gesamtprozess von CEO Fraud und über Präventionsmaßnahmen – insbesondere auch für das oft übersehene „Vorspiel" der Vorbereitungen. Wir gehen von den folgenden fünf Phasen aus: Recherche, Testing, Kontaktpflege, Angriff und Schaden.

Cyber Pairs
Dieses Serious Game bricht mögliche Barrieren auf und führt zu mehr Sicherheit im Umgang mit Begriffen bzw. Bezeichnungen von gängigen bzw. neuartigen Cybercrime-Angriffen, indem es dabei unter-stützt, diese auch im Detail zu verstehen und in Bezug auf mögliche Präventionsmaßnahmen unterscheiden zu können – stets verbunden mit der Fragestellung, was jede/r Einzelne von uns tun kann, um Risiken zu minimieren.

Mobile Kommunikation, Apps & Co.
Dieses Serious Game sensibilisiert in Bezug auf Risiken und Präventionsmaßnahmen, die die potenziellen Gefahren mobiler Kommunikation bzw. bei Nutzung von Apps verringern.

Daten- und Informationsschutz
Der Schutz von Informationen und Daten von Kund/innen, Mitarbeitenden und anderen Parteien ist Teil des Geschäftes jedes Unter-nehmen. Dieses Serious Game unterstützt dabei, Daten- und Informationsschutz zu gewährleisten, indem der Umgang mit den wichtigsten Schutzstrategien rekapituliert und eingeübt wird.

Infoklassen-Roulette
Der Zweck von Informationsklassifizierung ist der Schutz von wert-vollen Informationen jeder Organisation. Die „richtigen" Klassen hängen von den potenziellen Auswirkungen auf Verfügbarkeit, Beschädigung oder Verlust von Informationen ab. Dieses Serious Game unterstützt beim Verständnis von Informationsklassifizierung und deren Notwendigkeit.

Manövrieren Sie sich durch 7 Stories, jede eine Herausforderung für Wissen und Handeln.

Jedes Serious Game behandelt schwerpunktmäßig ein anderes für KMU informationssicherheits-relevantes Thema (z. B. Social Engineering, CEO-Fraud, Passwort-schutz). Die digitalen Serious Games können unabhängig voneinander und in beliebiger Reihenfolge gespielt werden.

Gleichwohl sind die einzelnen Geschichten durch eine übergreifende Gesamtstory, die in einem fiktiven KMU spielt, miteinander verknüpft.

https://alarm.wildau.biz/#learningScenarios

Ziel der digitalen Serious Games

In den digitalen Serious Games können Mitarbeitende die Themen der analogen Serious Games vertiefen und mit anderen Schwerpunkten erleben. Die digitalen Serious Games können aber auch unabhängig von den analogen absolviert werden, um das Bewusstsein für Informationssicherheit zu stärken.

Praxistipps – Konzepte die sie kennen sollten!

CEO-Fraud: Betrugsmethode über E-Mail als Kommunikationsmittel, bei der sich der Angreifer als Geschäftsführer, Manager oder Chef eines Unternehmens ausgibt.

Passwort Breach Service: Mithilfe der geschäftlichen E-Mailadressen wird geprüft, ob persönliche Identitätsdaten bereits im Internet veröffentlicht wurden und miss-braucht werden könnte.

Live-Hacking: Bildungs- und Informationsveranstaltung zur Entwicklung von persönlichem Risikobewusstsein und zur Sensibilisierung der Durchführung von Sicherheitschecks der IT-Infrastruktur auf organisatinaler Ebene.

Phishing: Beschaffung persönlicher Daten anderer Personen mit gefälschten E-Mails.

Smishing: Unter Smishing versteht man das betrügerische Ausspieonieren von sensiblen Daten per SMS.

Tailgating: Physischer „Einbruch" in das Unternehmen, um sensible Daten zu stehlen.

Vorfallsmeldung: Simulierter Ransomeware-Angriff mit dem Ziel den Incident Response Prozess in den Unternehmen zu aktivieren.

Sie wissen Bescheid?
Unser Security Self Chek könnte Sie verunsichern und/oder Wissenslücken aufdecken.

Sie können Ihr Wissen in allen Kategorien auf die Probe stellen und an den Ergebnissen anderer Anwender messen, die den gleichen Test ebenfalls absolviert haben.

https://sesec.wildau.biz

IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages

Homepage: https://alarm.wildau.biz

Prof. Dr. Margit Scholl (Projektmanagement):
margit.scholl@th-wildau.de

Abbildung 20 Zielerfüllung KNV: Neues Plakat zu den Ergebnissen des Projekts „ALARM Informationssicherheit" für die 13. Wildauer Wissenschaftswoche vom 11. bis 15. März 2024 (Download siehe Projektwebseite).

2.2.2 Gewonnene Erkenntnisse

Bereits in den vorherigen Kapiteln dieses Schlussberichts des Projekts „ALARM Informationssicherheit“ wurde auf die Komplexität des Projekts, die Herausforderungen durch die Corona-19-Pandemie und Wechsel bei Unterauftragnehmer und Personal hingewiesen. Gewonnene inhaltliche Erkenntnisse wurden ebenfalls an geeigneter Stelle skizziert. Zusammenfassend lässt sich feststellen (Scholl, 2024a):

Die Gefährdungssituation für deutsche KMU hat sich seit Beginn des Projekts nicht verbessert, sondern tendenziell ist sie so hoch wie nie zuvor. Mitarbeitende sind ein wesentlicher Bestandteil der Geschäftsprozesse von Unternehmen. Sie sind daher auch ein wesentlicher Bestandteil der Sicherheitsinfrastruktur dieser Prozesse, die die Existenz der Unternehmen darstellen. Mitarbeitende sind somit ein bedeutender Sicherheitsfaktor für KMU. Und wie auch technische Systeme mit Patches, Updates und Upgrades regelmäßig verbessert werden müssen, sind für Menschen Sensibilisierungs- und Schulungsmaßnahmen nicht nur sinnvoll, sondern auch regelmäßig notwendig und zudem eine durchaus kostengünstige Variante im Vergleich zu den Investitionen für technische Systeme. Der Einsatz von Technik ist für die Informationssicherheit unverzichtbar, aber ohne die Menschen wird ein Sicherheitsprozess nicht funktionieren bzw. nicht lebbar sein. Es ist somit eine ganzheitliche Betrachtungsweise von Informationssicherheit in den KMU zwingend erforderlich.

Bei der Entwicklung der analogen und digitalen Lernszenarien (Serious Games / realitätsnahe Simulationen) für Informationssicherheitsbewusstsein in KMU stellten wir fest, dass der Begriff „Gamification“ weitgehend unbekannt ist und zunächst erläutert werden muss. Danach war das Prinzip einsichtig und wurde bei den meisten Befragten als sinnvoll angesehen (Pokoyski et al. 2021). Es wird aber immer wieder sehr deutlich, dass das Spielerische bei Security Awareness in deutschen KMU nicht zu stark in den Vordergrund treten darf. Dies führt ansonsten zu deutlichen Widerständen bei den Sensibilisierungsmaßnahmen (Pokoyski et al. 2021).

Unsere Evaluationsergebnisse der entwickelten Lernszenarien sind zusammengefasst (Pokoyski & Hauke 2022):

- Gamifizierte Security Awareness in Form der entwickelten Serious Games wird von den Teilnehmenden ernst genommen. Sie werden als ein wichtiger Baustein der Informationssicherheit betrachtet und wirken zudem vitalisierend. D. h., im Spielen der Lernszenarien waren alle Teilnehmenden motiviert, gut gelaunt und konzentriert, und auch beim Feedback in der Nachbetrachtung waren alle bei der Sache.
- Es ist nach unseren Erfahrungen gelungen, Awareness-Maßnahmen mit Hilfe von Gamification auf ein Niveau zu heben, das Einbindung der Beteiligten schafft. Diese Sensibilisierungsleistung der Lernszenarien übersteigt die bisher üblichen lerntheoretischen Ansätze deutlich und funktioniert tatsächlich mit allen teilnehmenden Gruppen gut.
- Das im Projekt „ALARM Informationssicherheit“ für die Lernszenarien zugrunde liegende didaktische Konzept — „Talking Security“ — funktioniert auch in KMU reibungslos. Vor allem das diskursive Setting und die teamorientierten Interaktionen bei den analogen Lernszenarien fördern die Gespräche über „Situationen aus dem wahren Leben“ und bestätigen die Passung als Simulation realer Arbeits- und Alltagsszenarien.
- Unser diskursiver, teamorientierter Story-Telling-Ansatz wird auch international bestätigt.

Eine Security Awareness-Strategie war in KMU laut den Befragungen im Projekt „ALARM Informationssicherheit“ nur vereinzelt erkennbar und ist generell in KMU noch nicht etabliert – bestenfalls existiert eine gut gemeinte Absicht im Management und bei der Belegschaft. Allerdings würde die in Ansätzen in KMU vorhandene „Talking Security“ eine gute Möglichkeit bieten, eine solche Strategie zu entwickeln und auch nachhaltig vertreten zu können.

Unternehmen müssen dem Informationssicherheitsmanagement (ISM) zunehmend Priorität einräumen. Das Projekt „ALARM Informationssicherheit“ erzielt dazu als Gemeinschaftsprojekt und integrative Verzahnung unzweifelhaft hervorragende Ergebnisse. Jedoch haben wir bereits in der ersten Studie (Pokoyski et al. 2021) erkannt, dass die reine Bereitstellung von Online- oder analogen Awareness-Tools (Materialien) vermutlich nicht ausreichen wird. Viele Geschäftsführende und Führungskräfte benötigen Unterstützung bei der konkreten Ansprache ihrer Kunden und Mitarbeitenden, bei der nicht nur die jeweiligen Maßnahmen, sondern auch Idee und Intention dahinter im Kontext mit dem jeweiligen Geschäftsmodell präsentiert werden sollten (Pokoyski et al. 2021).

Geschäftsführende und Führungskräfte von KMU müssen die Nähe zum jeweiligen Kunden und den Mitarbeitenden für mehr Informationssicherheit nutzen und zugleich das gewünschte Sicherheitsverhalten der eigenen Organisation durch konsequentes Feedback steuern. Hierbei ist eine Form von Unterstützung nötig, die begleitend zu den geplanten Lernszenarien implementiert werden sollte (Pokoyski et al. 2021). Das Management und die Sicherheitstreibenden in den KMU müssen in Bezug auf Sensibilisierung erfahren lernen, dass nachhaltige ISA vor allem den diskursiven Effekt (Sprechen über Sicherheit) und damit die Auseinandersetzung mit den Mitarbeitenden benötigt. Dies umfasst auch die Art und Weise, Mitarbeitende produktiv anzusprechen. Eine entsprechende als neues Fokusprojekt beim BMWK eingereichte Projektskizze wurde jedoch nicht zur Bewilligung ausgewählt.

2.2.3 Beitrag zu den förderpolitischen Zielen

Alle Materialien und Leistungen berücksichtigen die betrieblichen Alltagsszenarien in deutschen KMU und sind umfänglich erprobt. In integrativer Verzahnung werden damit die folgenden Förderziele unterstützt:

- Sensibilisierung und Unterstützung von KMU und Handwerk beim Thema IT-Sicherheit im Zuge ihrer digitalen Transformation
- Stärkung von Wettbewerbs- und Innovationsfähigkeit von KMU durch den sicheren Einsatz digitalisierter Prozesse und Geschäftsmodelle
- Förderung technologischer, organisatorischer und arbeitsgestaltender IT-Sicherheitskompetenzen sowie Stärkung von Sicherheit und Vertrauen
- Erhöhung des IT-Sicherheitsniveaus in KMU durch Steigerung der Achtsamkeit und des Informationssicherheitsbewusstseins infolge von Sensibilisierungsmaßnahmen mit hochwertigen und erprobten Materialien
- KMU befähigen selbstständig kompetente IT-sicherheitsrelevante Entscheidungen zur Sensibilisierung und Schulung zu treffen.

3. Nutzen und Verwertung

3.1 Nutzen

3.1.1 known_sense

Die deutschen KMU unterscheiden sich trotz ähnlicher Probleme in Bezug auf die allgemeine Risikolage und trotz Ähnlichkeiten hinsichtlich der Risiken ihrer Sicherheitskultur deutlich von den Großunternehmen, die zu 90% den Kundenstamm der Firma known_sense bilden. Herkunft, Historie, Besitzverhältnisse, Führungskultur, (Security-)Reifegrad u.v.m. führte bei der Projektdurchführung zu besonders komplexen, hermetischen kulturellen Bedingungen, unter denen Awareness stattfinden soll. Diese Situation wird erschwert durch die vielfältigen Anforderungen an Menschen in den jeweiligen Führungs- bzw. Sicherheitsrollen, bei deren Ausfüllen es häufiger als in Großunternehmens zu Reibungsverlusten zwischen Führung und Ansprüchen der Sicherheit (unter dem Motto „Business vs. Defense“) kommt, so dass Sicherheitsmanagement und Sensibilisierung auch vor dem Hintergrund ganz unterschiedlicher Interessenskonflikten stattfinden.

Eine reibungslose, effiziente Nutzung diskursiver Awareness-Tools ist daher ohne vertiefende Erläuterung mit Methoden-Inkubation bzw. Begleitung durch Supervision und Coaching im KMU-Umfeld kaum realistisch.

Jedoch ist die KMU-Eigenperspektive hinsichtlich des hohen Bedarfs an wertiger (und damit geldwerter) Begleitung eher gering ausgeprägt. Da nachhaltige Awareness nicht zum Nulltarif oder „low budget“ möglich ist und die Bereitschaft von deutschen KMU, in die Modellierung von Sicherheitskultur und Awareness jenseits von Gratis-Formaten zu investieren, offenbar immer noch sehr gering ist, wird sich die Firma known_sense auch künftig mit ihren Angeboten eher an Konzerne wenden, denn ohne Fördermittel ist die Durchsetzung nachhaltiger Awareness in KMU aus der Projekterfahrung nur schwerlich möglich. Der Kundenstamm der Firma verbleibt somit i.d.R. bei großen Unternehmen.

Für den „Awareness-Koffer“ mit den hochwertig produzierten Materialien gibt es regelmäßig Anfragen, die jedoch i.d.R. außerhalb von KMU liegen. Diese Anfragen werden gegen Bezahlung von dem Unterauftragnehmer known_sense erfüllt.

Da die entwickelten analogen Serious Games laut tiefenpsychologischer Tests des Projekts „ALARM Informationssicherheit“ sehr gut funktionieren, ist known_sense bereits dabei, Content-Fragmente aus dem Projekt entsprechend der sich verändernden Risikolandschaft und des sich entwickelnden Bedarfs weiterzuentwickeln und ihren Kunden anzubieten – durchaus auf lange Sicht mit immer besserer zielgruppenorientierter Passung und einem wachsenden Reifegrad. Gleichzeitig kommen auch Neukunden aus Organisationen jenseits von internationalen Konzernstrukturen auf die Firma zu – im Wesentlichen technologische Weltmarktführer mit hohem, Schutzpotenzial ihrer Produkte bzw. Patente, die allerdings mit ihren Mitarbeitendenzahlen ebenfalls noch deutlich über der KMU-Definition liegen.

3.1.2 Gamebook Studio GmbH

Das Unternehmen Gamebook Studio GmbH hat seine Beteiligung an dem Projekt „ALARM Informationssicherheit“ genutzt, um sich besser zur Information Security aufzustellen und innerhalb ihres Geschäftsmodells, der Erstellung digitaler Serious Games, erweitert zu positionieren. Gamebook Studio hat die erarbeiteten deutschen Serious Games unseres Projekts in englischsprachige Versionen transferiert, um diese am Markt neu anzubieten. Insofern verspricht sich das Unternehmen damit einen deutlichen Nutzen an neuer Marktpräsenz für bezahlte Dienstleistungen auf dem Gebiet der digitalen Spieleentwicklung (s. Abb. 19).

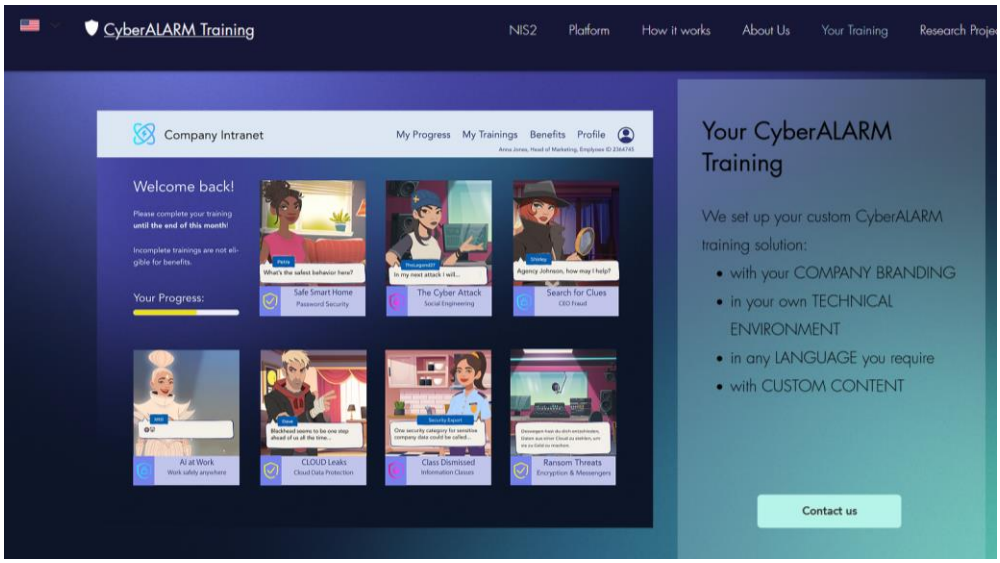


Abbildung 21 Neuer Geschäftsimpuls durch das Projekt „ALARM Informationssicherheit“ für das Unternehmen Gamebook Studio GmbH. Quelle: https://www.cyberalarm.training/, Stand: 18. März 2024.

3.1.3 Thinking Objects (TO) GmbH

Der Unterauftragnehmer TO weist eine breite Palette von sicherheitsrelevanten Dienstleistungen für KMU auf; seine Expertise lieferte niederschwellige Sicherheitskonzepte aufgrund der durchgeführten „Vor-Ort-Angriffe“. TO verdeutlichte allen Akteuren im Projekt, wie bedeutsam die vertrauensvolle Zusammenarbeit mit der KMU-Geschäftsführung und den Mitarbeitenden ist, um überhaupt Vor-Ort-Angriff-Simulationen sinnvoll durchführen zu können. Die weiteren kostenfreien Ergebnisse des Projekts bringt TO in seinen Kundengesprächen aktiv ein.

Das Projektdesign mit den verschiedenen Schwerpunkten auf analoge, digitale und erlebnisorientierte (Vor-Ort-Angriffe) Sensibilisierung für Cyberangriffe hat TO deutlich gezeigt, wie wichtig es ist, unterschiedliche Vermittlungsmethoden für eine nachhaltige Awareness anzubieten, um möglichst viele Mitarbeitende in Unternehmen und Organisationen zu erreichen. TO strebt eine weitere Zusammenarbeit vor allem mit known_sense und Gamebook Studio GmbH an.

3.1.4 sudile GbR

Das Material des Projekts „ALARM Informationssicherheit“ zu sicherheitsrelevanten Themen wird dem zentralen IT-Dienstleister des Landes Brandenburg (ZIT BB) für seine interne Lehrlings-Ausbildung erläutert. Die Firma sieht dies unter „kostenfreie Kontaktpflege“.

Die Datenbank, auf die der Selbsttest (SeSec) zugreift, wird von sudile weiterhin und kostenfrei bis 2027 gepflegt. Ebenso wird die Aktualisierung der Kalenderblätter auf das jeweils nächste Jahr kostenfrei betreut. Die Firma verspricht sich als Nutzen eine Steigerung der Aufmerksamkeit für diese Produkte.

3.1.5 TH Wildau (Zuwendungsempfängerin und Projektkoordinatorin)

Die TH Wildau konnte ihren Ruf als praxisorientierte Forschungsstätte mit hochwertiger, moderner Lehre durch das Projekt „ALARM Informationssicherheit“ national und international ausbauen. Intern werden Studierende und Mitarbeitende mit den Materialien des Projekts sensibilisiert. Ebenso profitieren die Events und externe Fort- und Weiterbildungssektor der Hochschule, indem auf die Ergebnisse verwiesen werden kann. Die TH Wildau hat darüber hinaus ihre Projektmanagementfähigkeiten anhand des komplexen Projektes auch außenwirksam erneut bewiesen.

Das komplexe Projekt war für alle Beteiligten eine äußerst herausfordernde Situation, zumal die Corona-Pandemie noch erschwerend dazu kam. Mit den erreichten Projektergebnissen und allen Veröffentlichungen hat das Team diese Aufgabe letztlich souverän gemeistert. Bereits vor, aber spätestens mit dem ursprünglich geplanten Ende des Projekts „ALARM Informationssicherheit“ haben die kompetenten Projektmitarbeitenden attraktive Jobalternativen erhalten oder sind in eine freiwillige „Entschleunigungszeit“ mit besserer Work-Life-Balance eingetreten. Die Finanzierung eine projektbezogenen Anschluss- und Weiterförderung ist derzeit nicht gegeben.

3.2 Für die Region / Branche

Wie in Scholl (2024a) ausgeführt, wurde bereits in der ersten Studie des Projekts „ALARM Informationssicherheit“ darauf hingewiesen, dass Security Awareness als Teil von Sicherheitskommunikation eine Voraussetzung für erfolgreiches Sicherheitsmanagement in KMU darstellt und sicherheitsrelevantes Verhalten der Beschäftigten positiv beeinflusst (Pokoyski et al. 2021). Daher reduziert die kontinuierliche Implementierung von Maßnahmen zur Erhöhung des Informationssicherheitsbewusstseins der Mitarbeitenden in überprüfbarer Weise nicht nur das

geschäftliche Risiko von Unternehmen, sondern sie erhöht darüber hinaus deren Attraktivität (Pokoyski et al. 2021). Denn sowohl die Zusicherung solcher Maßnahmen gegenüber den Kunden mit veränderter externer Kommunikation als auch die Erfüllung von gesetzlichen Auflagen oder internationalen Sicherheitsstandards sichern den Unternehmen mit einem aktiven Sicherheitsmanagement auch Wettbewerbsvorteile, da sie positive Imagefaktoren generieren und das Vertrauen in das Unternehmen erhöhen (Pokoyski et al. 2021). Somit etabliert sich Security Awareness zunehmend als ein Reputationsinstrument, das den Vertrauensgrad zwischen Dienstleister und Kunde zu beeinflussen vermag (Pokoyski et al. 2021).

Der von dem Projekt „ALARM Informationssicherheit“ initiierte und erreichte Methoden-Mix erweitert für KMU die in der Praxis erprobten einsetzbaren Sensibilisierungsmöglichkeiten in einer integrativ verzahnten Art und Weise, so dass eine nachhaltige Reputation durch steigende Informationssicherheit in deutschen KMU aufgebaut werden kann.

Da das Projekt mit Unternehmenspartnern und Pilotunternehmen überregional ausgelegt war und die Veranstaltungen des Forschungsteams bis März 2024 in unterschiedlichen Bundesländern stattfanden, konnte zudem ein regionübergreifender Austausch zwischen den Projektbeteiligten und interessierten Akteuren gesichert werden. Dies hat von Beginn an eine breitenwirksame Bekanntheit der Projektziele initiiert. Darüber hinaus hat die TH Wildau und damit auch das Land Brandenburg an Bedeutung für betriebliche Information Security Awareness gewonnen, vor allem auch, da die Projektziele mit konkreten qualitativ hochwertigen Produkten erreicht wurden, die kostenfrei über die Projektwebseite für nicht-kommerzielle Nutzung zur Verfügung stehen. Diese werden zudem von Institutionen, die keine KMU darstellen, zunehmend genutzt: beispielsweise bindet die Brandenburger Polizei die Lernszenarien des Projekts in ihre eigene interne Sensibilisierungskampagne ein, so dass inzwischen auch die Polizei Berlin und das Landeskriminalamt Mecklenburg-Vorpommern Interesse an den existierenden Lernmaterialien gezeigt haben.

3.3 Verwertung / Nachhaltigkeit

3.3.1 Weiterführungsmöglichkeiten

Die Herausforderungen im Projekt waren vielfältig, durch die Covid-16-Pandemie stark beeinträchtigt und auch geprägt von einem immer wiederkehrenden Personalwechsel in dem komplexen Projekt „ALARM Informationssicherheit“:

- Über die drei Jahre Projektdauer gesehen, wurde der verbundene Aufwand innerhalb der Pilot-KMU als zu hoch angesehen. Als agile Unternehmen mit knappen Ressourcen, die am Markt bestehen müssen, wurde zunehmend die Forderung laut, für die eigene Beteiligung selbst eine finanzielle Förderung erhalten zu müssen. Dies war allerdings im Förderprogramm des BMWK ursprünglich nicht vorgesehen.
- Unsere Erfahrungen mit den Pilot-KMU lassen vermuten, dass in einem Folgeprojekt die KMU noch konkreter betreut und an die Hand genommen werden müssen, um eine nachhaltige Sensibilisierungsstrategie zu entwickeln und kontinuierliche Sensibilisierungsmaßnahmen in den relevanten Geschäftsprozessen zu etablieren. Dieser Betreuungsbedarf der KMU bedeutet die Berücksichtigung von noch mehr Personalkosten für ein durchführendes zukünftiges Projektteam.
- Der geleistete Beitrag des Projekts „ALARM Informationssicherheit“ wäre ohne das äußerst engagierte Forschungsteam der TH Wildau, das nur über befristete Teilzeit-Projektverträge finanziert werden konnte, nicht möglich gewesen.
- Inhaltlich müssen wir von einer sehr deutlichen sicherheitskulturellen Bandbreite in den deutschen KMU und von einer deutlich unterschiedlichen Ausprägung des Awareness-Reifegrads ausgehen, so dass die einzelnen Lernszenarien nicht überall gleich gut wirken. Jedoch gibt es bei den im Projekt „ALARM Informationssicherheit“ entwickelten analogen Serious Games einen großen Vorteil (Pokoyski & Hauke, 2022): Ihr auf Differenzierung ausgelegter modularer Ansatz mit der Möglichkeit individueller Adaptierbar-

keit unterstützt die KMU, diese große Bandbreite für sich selbst in den Serious Games durch eigene praktische Beispiele zu ergänzen und damit praxisorientiert anzupassen.
- Die Übertragbarkeit der Serious Games auf andere Bereiche wird in der Projektdokumentation (Scholl, 2024a) skizziert, so dass prinzipiell Weiterführungsmöglichkeiten auch in anderen Zusammenhängen bestehen, sei es im Gesundheitswesen und Krankenhäusern, sei es in Landesverwaltungen und Kommunen, sei es in Studiengängen an Hochschulen und Universitäten.
- Leider konnten die Awareness-Messungen und Reifegrad-Bestimmungen als Folge der Überlegungen zur Wirkung der Lernszenarien in quantitativer Form durch die verantwortliche Projektmitarbeiterin nur rudimentär innerhalb des Projekts „ALARM Informationssicherheit“ durchgeführt werden. Ein kurzer Abriss unserer Erkenntnisse wird in Scholl (2024a) gegeben, mit dem Resultat, dass dieser Themenkomplex in weiteren neuen Forschungsprojekten behandelt werden muss, denn es ist ein noch offenes, komplexes Forschungsgebiet. Hinsichtlich der Awareness-Messungen und Reifegradaussagen sind viel intensivere Forschungen nötig, um qualitativ hochwertige Ergebnisse liefern zu können. In der Projektdokumentation (Scholl, 2024a) können daher nur Tendenzen der Bewusstseinsveränderung skizziert werden. Andere Forschungsgruppen sind hier intensiv an der Entwicklung von Modellen, deren Praxistauglichkeit allergings noch aussteht. Die verantwortliche Projektmitarbeiterin im Projekt „ALARM Informationssicherheit“ hatte vor, ihre Masterarbeit mit dem Thema zu absolvieren.

3.3.2 Wirtschaftliche Verwertung durch die Projektpartner

Die wirtschaftlichen Erfolgsaussichten der Ergebnisse im Berichtszeitraum haben sich gegenüber dem Projektantrag als unverändert erwiesen und konnten durch folgende Maßnahmen des Projekts bestätigt werden:
- Serious Games sind hochaktuell und werden in verschiedensten Themengebieten eingesetzt.
- Die Methode Gamification findet in der Gesellschaft und in deutschen Unternehmen immer mehr Zuspruch.
- Durch die konkrete Präsenz des Themas Informationssicherheit in den Pilot-KMU infolge der Aktivitäten des Projekts „ALARM Informationssicherheit“ ist bereits jetzt davon auszugehen, dass deren Mitarbeitenden mehr für Informationssicherheit sensibilisiert sind.
- Im großen Rahmen sehen sich die deutschen KMU jedoch nach wie vor offenbar nicht in der Lage, dafür monetäre Beträge zu bezahlen und in die notwendigen Ressourcen (Personal und Zeit) zu investieren.

Die aktuelle Forschungslage zu Gamification ist eine Bestätigung für unser Projekt. Die Unterauftragnehmenden werden vermutlich ihre Geschäftsmodelle in diese Richtung stärken. Ob dies allerdings ohne neue Fördermittel mit KMU gelingt bleibt unklar:
- Der Bekanntheitsgrad bzw. die Netzwerkkultur des Unterauftragnehmers known_sense war bereits vor dem Projekt ausgeprägt. Die Firma hat nicht das Gefühl, dass dies durch das Projekt in Richtung KMU weiter gesteigert werden konnte. Einen wirtschaftlichen Benefit muss die Firma selbst durch die Umsetzung der Erfahrungen aus dem Projekt erarbeiten. Dies geschieht auch basierend auf den o. g. Content-Fragmenten, die innerhalb von modularen Remixen anschlussfähig an den Markt sind.
- Für Gamebook Studio GmbH werden neue Projekte für digitale Serious Games im Bereich Informationssicherheit durch etliche Nachfragen wahrscheinlich, allerdings nicht unbedingt aus dem KMU-Sektor, sondern vielmehr aus dem Bereich der öffentlichen Verwaltung, Gesetzgebung und Sicherheit. Aktuell entwickelt Gamebook Studio eine eigene neue Plattform, die ein Schulungsangebot im Kontext der im Jahr 2024 in Kraft tretenden NIS2 Regularien für Unternehmen in ganz Europa schaffen soll. Insofern verspricht sich das Unternehmen damit eine deutliche neue wirtschaftliche Verwertung. Weiterhin prüft das Unternehmen aktuell auch eine Erweiterung des Angebots im Rahmen von Bildungsprogrammen für eine jüngere Zielgruppe.

- Der Unterauftragnehmer Thinking Objects (TO) GmbH war bereits vor dem Projekt am Markt und bei KMU mit seinem stabilen Sicherheitsgeschäftsmodell bekannt. Einen wirtschaftlichen Benefit aus dem Projekt muss das Unternehmen selbst erst durch die Umsetzung der Erfahrungen aus dem Projekt erarbeiten; Inspiration hat das Projekt dazu gegeben: Ausgewählte Vor-Ort-Angriffe sind bereits Bestandteil ihres Awareness Portfolios und auf Grundlage der Projektergebnisse werden diese kontinuierlich weiterentwickelt. TO nutzt ebenfalls die Möglichkeit, ihren Kunden die bestehenden Angebote von known_sense und Gamebook Studio vorzustellen; ggf. werden sich neue wirtschaftliche Kooperationen ergeben.
- Die kleine Firma sudile gbR sieht derzeit für sich und ohne neue Fördermittel keine weitere wirtschaftliche Verwertung des Erreichten.

3.3.3 Wissenschaftliche Verwertung durch die Projektpartner

Im Projekt „ALARM Informationssicherheit“ wurde von Beginn an eine sehr aktive wissenschaftliche Verwertung betrieben und auch hier im Schlussbericht dokumentiert (s. Kapitel 2.2.1 und Anlage 4).

Die drei im Rahmen des Projektes von known_sense erstellten Studien weisen auf die Besonderheiten im deutschen KMU-Umfeld hin. Wir sehen damit, dass die im Projekt „ALARM Informationssicherheit“ kreierten Serios Games und weiteren Materialien/Tools mit hohem Impact in Organisationen aller Art funktionieren und Awareness hierdurch auf ein höheres Reifegradniveau gehoben wird.

Jedoch bleibt das Problem für die TH Wildau und die Mehrheit der Unterauftragnehmer bestehen, dass die KMU in absehbarer Zeit ohne Fördermittel im großen Rahmen keine eigenständige bezahlende Zielgruppe für praxisnahe Forschung und betriebliche Anwendung im Bereich Security Awareness darstellen.

Der Unterauftragnehmer Gamebook Studio GmbH sieht seine Arbeit im Projekt „ALARM Informationssicherheit“ trotzdem sehr positiv, da dies für ihn einen wichtigen Anknüpfungspunkt bot, um einen aktuellen Überblick zu den politischen, wirtschaftliche und akademischen Akteuren im Bereich Information Security am Markt zu erhalten und das eigene Netzwerk in diesem Bereich zu erweitern. Insbesondere die Beteiligung an Veranstaltungen der TH Wildau und Netzpartnern sowie an den wissenschaftlichen Publikationen des Projekts hat einen wichtigen Anschlusspunkt für das Unternehmen sowie dessen Sichtbarkeit für die eigenen Forschungsaktivitäten in der technischen Entwicklung gegeben.

3.3.4 Anschlussfähigkeit

Das Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ zeigt mit hervorragenden Ergebnissen auch verbleibende KMU-Defizite vor allem in drei Bereichen auf (Scholl, 2024a):

- Die Bereitstellung von qualitativ und didaktisch hochwertigen Sensibilisierungsmaterialien für Mitarbeitende in KMU reicht nicht aus, um sicherzustellen, dass KMU diese tatsächlich innerbetrieblich nutzen; vielmehr müssen KMU intensiver begleitet werden, um einen nachhaltigen Transfer zu gewährleisten.
- Dies bedeutet zum einen, dass Moderatoren und Moderatorinnen für die Sensibilisierungsmaßnahmen in KMU ausgebildet werden sollten („Awareness-Beauftragte bzw. -Beauftragter“); diese können intern im KMU rekrutiert werden oder extern über Beratungsfirmen einbezogen werden. Die Qualität der Moderation hängt wiederum von einer guten Ausbildung ab, die über eine anerkannte Zertifizierung sichergestellt werden sollte.
- Des Weiteren sind ein entscheidender Faktor für die erfolgreiche Sicherheitskommunikation innerhalb eines KMU sein TOP-Management (Geschäftsführende) und seine

Führungskräfte; hier können auch externe Beratungsunternehmen eine entscheidende Transferfunktion übernehmen. Allerdings benötigt eine solche Unterstützung zur Selbsthilfe der KMU bzw. ein solches Coaching andere Materialien für Führungskräfte als die bislang entwickelten Sensibilisierungsmaßnahmen für Mitarbeitende.

Es bleibt abschließend für ein neues Awareness-Projekt in KMU festzuhalten, dass eine anwendungsorientierte Unterstützung des Top-Managements und ein erlebnisorientiertes Coaching der Führungskräfte notwendig ist. Dies bedeutet auch eine zentrale Neuausrichtung und Entwicklung von entsprechenden Tools für Führungskräfte, deren Fokus auf die interne Sicherheitskommunikation und die Risikowahrnehmung gerichtet sein muss. Da das von uns neu eingereichte Fokusprojekt jedoch bislang nicht bewilligt wurde, besteht für die TH Wildau derzeit keine Anschlussfähigkeit des Projekts „ALARM Informationssicherheit“.

Auch für die Unterauftragnehmer wäre es interessant und zielführend gewesen, ein Folgeprojekt bewilligt zu erhalten, in dem wir gemeinsam spezifizierte Formate für Führung (Top-Management und Führungskräfte) und Security-Rollen hätten begleiten können, sei es mit Methoden-Inkubation, Supervision, Coaching u.v.m. sowie durch neue bildhafte Tools. Vermutlich hätte ein derartiger Prozess und eine daraus resultierende Unterstützungsexpertisé zur Selbsthilfe speziell für das Management zu einer nachhaltigeren Implementierung und Nutzung diskursiver Formate in KMU führen können als es jetzt vermutlich der Fall sein dürfte. Ohne neue Fördermittel sehen wir uns jedoch nicht in der Lage, derartige Projekte für das KMU-Management anzustoßen, selbst zu finanzieren und durchzuführen.

4. Anlagen

4.1 Veröffentlichungen (Liste)

2021

Pokoyski, D., Matas, I., Haucke, A. & Scholl, M. (2021). *Qualitative Wirkungsanalyse Security Awareness in KMU* (Projekt "ALARM Informationssicherheit") (p. 72). Wildau: Technische Hochschule Wildau. Download: https://alarm.wildau.biz/ (**Studie 1**)

Scholl, M. (2021a). Foreword with an Introduction to and Summary of the Study “Added Value for SMEs” (Translation). doi:10.13140/RG.2.2.21236.88961

Scholl, M. (2021b). *Informationssicherheit mit (!) Führungskräften*. Presented at the Runder Tisch für Cybersicherheit im vorpolitischen Raum beim BSI. Download: https://www.th-wildau.de/files/Beschaeftigte/Margit_Scholl/210617_Impulsvortrag_RunderTisch_final.pdf

Scholl, M., Schuktomow, R., & Gube, S. (2021). Information security in pandemic times—a discussion paper. (International Insitute of Systemics, Cybernetics, and Informatics: IIIS), *Proceedings of the 25th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2021)*. Florida, USA: International Institute of Informatics and Systemics (IIIS). Retrieved from https://www.iiis.org/CDs2021/CD2021Summer/papers/DW756AS.pdf

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2021). Global Cybersecurity Index (GCI) and the Role of its 5 Pillars. *Social Indicators Research*, *159*, 125–143. doi:10.1007/s11205-021-02739-y

Scholl, M., & Schuktomow, R. (2021). The Current State of "Information Security Awareness" in German SMEs. *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, *11*(12), 151–163. doi:10.46338/ijetae1221_16

2022

Scholl, M. (2022a). ALARM INFORMATIONSSICHERHEIT. *TAKE AWARE SEC&LIFE Magazine*. unbekannt: unbekannt. Download: https://www.take-aware-events.com/storage/app/media/pdf/takeawaresecandlifemagazine05.pdf

Pokoyski, D. & Haucke, A. (2022). *Enabling vs. Entmündigung*. Scholl, M. (Ed.) (2022b), Wildau: TH Wildau. Download: https://alarm.wildau.biz/static/c0e4d00beefe1dc5fac9b50b6087265f/studie-2-master-final.pdf (**Studie 2**)

Scholl, M. (Ed.). (2022c). Entwicklung von erlebnisorientierten Lernszenarien zur Sensibilisierung für Informationssicherheit. Presented at the 11. Wissenschaftswoche der TH Wildau. doi:10.13140/RG.2.2.19209.52323

von Tippelskirch, H., Schuktomow, R., Scholl, M., & Walch, M. C. (2022). *Report zur Informationssicherheit in KMU – Sicherheitsrelevante Tätigkeitsprofile (Report 1)* (p. 111). Wildau: TH Wildau. Retrieved from https://alarm.wildau.biz/static/3b60581edae4d016e4c20290c0936f55/220623_alarm_report1_web.pdf (**Report 1**)

Scholl, M. (2022d). Foreword and Reflection on the Findings Contained in Report 1 of the Project Awareness Lab SME (ALARM) Information Security. doi:10.13140/RG.2.2.13075.35363
Scholl, M., Schuktomow, R., & Mujkic, O. (2022). Projekt "Awareness Labor KMU (ALARM) Informationssicherheit" Presented at the 11. Wissenschaftswoche der TH Wildau. doi:10.13140/RG.2.2.36406.16965

Prott, F., & Scholl, M. (2022a). Raising Information Security Awareness Using Digital Serious Games with Emotional Design. *IADIS International Journal on WWW/Internet*, *20*(2), 18–34.

Prott, F., Küchler, U., Schuktomow, R., & Scholl, M. (2022). Serious Games als Lernmethode zur Steigerung der Informationssicherheit. (S. Eggert, C. Lemke, V. Majuntke, B. Malzahn, V. Meister, K. Simbeck, … M. Wolf), *Angewandte Forschung in der Wirtschaftsinformatik 2022*. Berlin: GITO mbH. doi:10.30844/AKWI_2022_23

Prott, F., & Scholl, M. (2022b). Using Emotional Design to Raise Awareness of Information Security. (K. Blashki), *Proceedings of the International Conferences on Interfaces and Human Computer Interaction 2022 and Game and Entertainment Technologies 2022*. Lissabon: IADIS Press. Download: http://www.iadisportal.org/digital-library/using-emotional-design-to-raise-awareness-of-information-security

von Tippelskirch, H., & Scholl, M. (2022a). Tailored Information Security Training: Identification of Target Groups in German SMEs Based on Job Profiles. (Ungeklärt), *London International Conference on Education (LICE-2022) and World Congress on Special Needs Education (WCE-2022)*. London: Infonomics Society.

von Tippelskirch, H., & Scholl, M. (2022b). Target Groups in German SMEs for Information Security Training: The Use and Limits of Job Profiles in Designing Training Units. *Journal of Internet Technology and Secured Transactions*, *10*(1), 787–795. doi:10.20533/jitst.2046.3723.2022.0097

2023

Pokoyski, D., Haucke, A., & Scholl, M. (2023). *Game over vs. Game Lover* (1st ed.) (p. 63 Seiten). Wildau: Technische Hochschule Wildau. Download: https://alarm.wildau.biz/static/0fa10a2f646ddcc06fb36d5636a5025f/Studie3_final.pdf (**Studie 3**)

Scholl, M. (2023a). Chapter 5 Findings from the overall scenario and the three studies of the project “Awareness Lab SMEs (ALARM) Information Security” followed by a conceptual outlook. Wildau: Technische Hochschule Wildau. doi:10.13140/RG.2.2.12630.22082

von Tippelskirch, H., Prott, F., & Scholl, M. (2023). *Gemeinsam zum Projekterfolg* (p. 16 Seiten). Wildau: TH Wildau. Download: https://alarm.wildau.biz/static/6481a77fec203f00a077ed2cdd049f1f/report3-final.pdf (**Report 3**)

Bruggemann, R., Koppatz, P., Carlsen, L., & Scholl, M. (2023). Cyberattacks: An Attempt to Obtain a Multidimensional Awareness Indicator. doi:10.13140/RG.2.2.29494.88642

Schuktomow, R., von Tippelskirch, H., & Scholl, M. (2023). Informationssicherheit in den Arbeitsalltag nachhaltig integrieren: Informationssicherheitskultur verstehen, mit Serious Games sensibilisieren und das Informationssicherheitsbewusstsein der Mitarbeitenden erhöhen. (C. Czarnecki, A. Lübbe, V. G. Meister, C. Müller, M. Steglich, & M. Walther), *Angewandte Forschung in der Wirtschaftsinformatik 2023: Tagungsband zur 36. AKWI-Jahrestagung vom 11.09.2023 bis 13.09.2023 ausgerichtet von der Technischen Hochschule Wildau*. Wildau: Technische Hochschule Wildau. doi:10.15771/1794 (**Report 2**)

Scholl, M., Schuktomow, R., Tippelskirch, H. von, Prott, F., Pokoyski, D., Vogt, M., … Koppatz, P. (2023). *Präsentation der Ergebnisse des Projekts "ALARM Informationssicherheit"* / Presented at the Awareness Forum 2023. doi:10.13140/RG.2.2.35979.46887

Scholl, M. (2023b). Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect. (University of Hawai’i at Manoa), *Proceedings of the 56th Hawaii International Conference on System Sciences*. Honolulu, HI: University of Hawai’i at Manoa, Hamilton Library. URI: https://hdl.handle.net/10125/103369, (CC BY-NC-ND 4.0), 6058-6067

Scholl, M. (2023c). German SMEs & “Home Office”: Narrative-Driven Game-Based Awareness Raising with Long-Term Efficacy. In S. Mistretta, *Reimagining Education - The Role of E-learning, Creativity, and Technology in the Post-pandemic Era* (pp. online ca. 36 Seiten). London: IntechOpen. doi:10.5772/intechopen.1003002

Scholl, M. (2023d). Raising Awareness of CEO Fraud in Germany: Emotionally Engaging Narratives Are a MUST for Long-Term Efficacy. (Álvaro Rocha, C. Ferrás, & W. Ibarra), *Information Technology and Systems*. Cham: Springer International Publishing. doi:10.1007/978-3-031-33258-6_40

2024

Scholl, M. (Ed.). (2024a). Neue Wege für mehr Informationssicherheit in KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit. Frankfurt/M.: Buchwelten Verlag.

Scholl, M. (2024b). Summary of the project documentation “Awareness Lab SME (ALARM) Information Security” doi:10.13140/RG.2.2.20336.64002/1

Scholl, M. (2024c). Résumé of the Gamified Increase in Security Awareness in German Small and Medium-Sized Businesses after Three Years' Practice of "ALARM Information Security" doi:10.13140/RG.2.2.13519.29600

Scholl, M. (2024d). Schlussbericht des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit": Neue Wege für mehr Informationssicherheit in deutschen KMU. Wildau: TH Wildau.

Scholl, M. (2024e). Building Competence with a Targeted Mix of Analog and Digital Methods. In L. Willyanto Santoso, *Contemporary Perspective on Science, Technology and Research* (pp. 35 & ndash;58). Kolkata: B P International. doi:10.9734/bpi/cpstr/v5/8542A

Scholl, M. (2024f). Play the Analog Game in a Digital World! Long-Term Gamification for Raising Information Security Awareness. In L. Willyanto Santoso, *Contemporary Perspective on Science, Technology and Research* (pp. 19–43). Kolkata: B P International. doi:10.9734/bpi/cpstr/v6/8543A

Scholl, M. (2024g). Awareness Labor KMU (ALARM) Informationssicherheit. In: Forschungs-/Transferbericht TH Wildau 2023. Veröffentlichung vermutlich im April / Mai 2024 mit doi: 10.15771/BFT_2024.

4.1.1 Buch-Cover Abschlussdokumentation auf Deutsch:

Scholl, M. (Ed.). (2024a). *Neue Wege für mehr Informationssicherheit in KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit.* Frankfurt/M.: Buchwelten Verlag.

Abbildung 22 Buch-Cover der Projektdokumentation als zugrundeliegende Abschlussdokumentation des Projekts „ALARM Informationssicherheit" bis 30. September 2023.

ALARM BUCH, EPUB & PDF

https://buchwelten-verlag.de/ebooks.php

"978-3-945740-75-0","Buch"
"978-3-945740-76-7","EPUB"
"978-3-945740-77-4","PDF"

4.1.2 Zusammenfassung Projektdokumentation auf Englisch

Scholl, M. (2024b). Summary of the project documentation “Awareness Lab SME (ALARM) Information Security” doi:10.13140/RG.2.2.20336.64002/1.

Veröffentlicht als Experimental Findings:

DOI: 10.13140/RG.2.2.20336.64002

Summary of the project documentation
“Awareness Lab SME (ALARM) Information Security”
(in English)

Margit Scholl

Technical University of Applied Sciences Wildau (TH Wildau)

Foreword

People are being hacked: What to do?

It takes a lot of perseverance to realize a complex project idea, such as the practice-oriented research project “Awareness Lab SME (ALARM) Information Security.” The idea of holistic and innovative support for greater information security awareness in small and medium-sized companies (SMEs) was born in a brainstorming session involving the managing director of Thinking Objects, Markus Klingspor, and me—a professor with an active research profile at the Technical University of Applied Sciences Wildau (TH Wildau)—at an event on the cyberthreat situation in Germany in 2016. The idea was then made more concrete when the team expanded to include the manager of the firm known_sense, Dietmar Poykoski, a long-time associate in my security projects on innovative learning and teaching methods at TH Wildau.

After numerous revisions, the project outline, which was ultimately developed with the involvement of additional subcontractors and associated partners, was submitted in February 2019. With positive feedback, the actual project application was submitted in October 2019 to the “IT Security in Business H2” funding guideline of the Federal Ministry for Economic Affairs and Climate Protection (BMWK) via the German Aerospace Center (DLR). The detailed application title was: “Awareness Lab SME (ALARM): Interactive, tangible personnel development for more information security and organization-wide security analyses in SMEs” (Scholl 2019). After further inquiries had been clarified, the time had come in 2020: in June, TH Wildau received the funding notice for a project running from October 1, 2020, to September 30, 2023. Through economical project management, a cost-neutral extension of the project with a few staff hours was feasible through to March 31, 2024, so that all results can continuously be improved and made widely known.

The complexity of the practice-oriented “ALARM Information Security” project was clear from the start, as it was intended to develop an overall scenario to raise awareness and support SMEs for information security through to self-help within just three years. The underlying research design mainly contained new developments within a central project management control, which were carried out iteratively in three agile and participatory phases, an innovative process scenario for information security with analog and digital experience-oriented scenarios as well as “on-site attacks” and other checks, such as awareness measurements, quizzes, and tests. The aim of the overall scenario was to promote the urgently needed operational awareness raising of executives and employees and

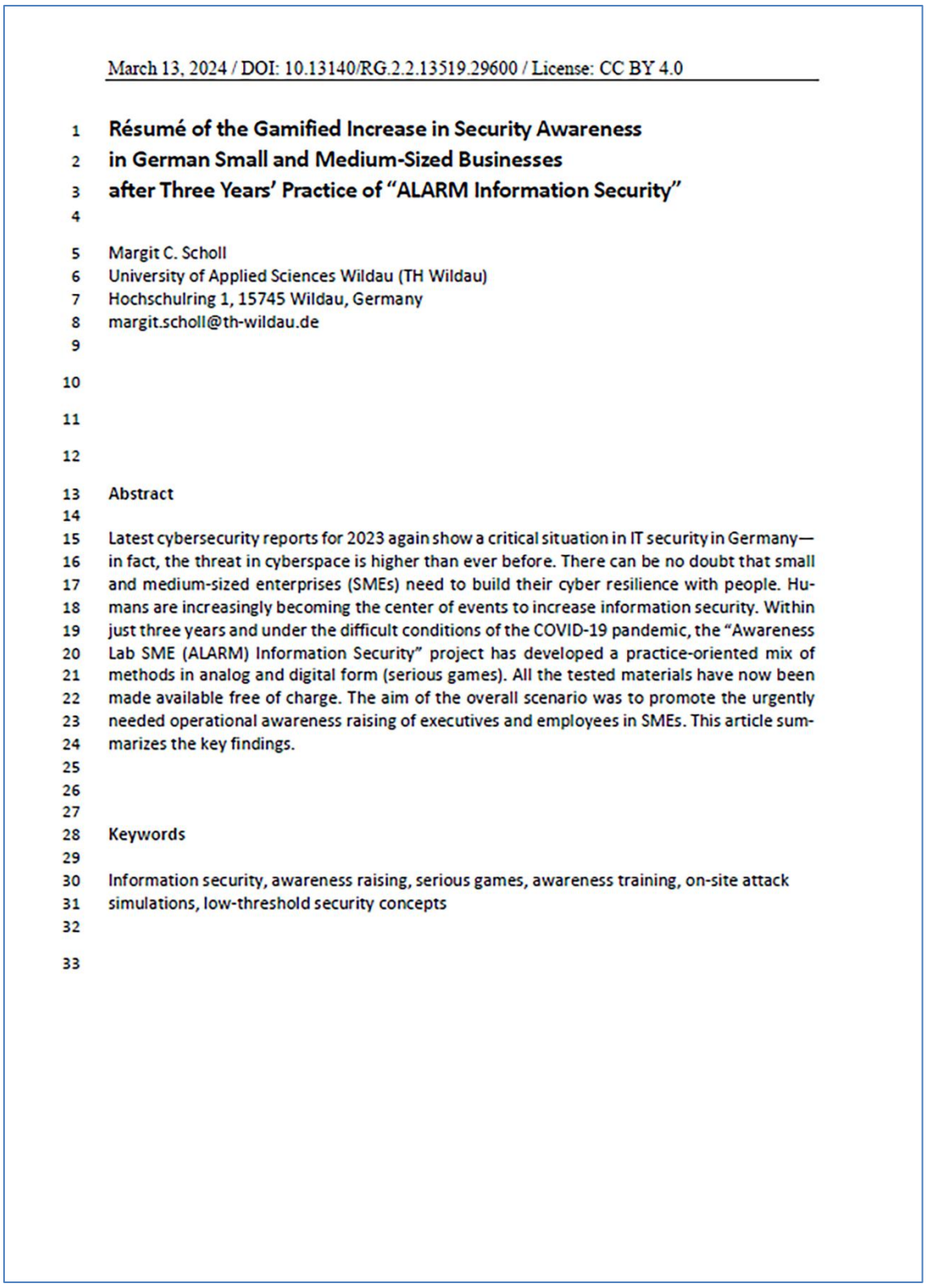
CC BY-SA 4.0 of this summary in English 1 published in February 2024

Abbildung 23 Erste Seite der englischsprachigen Zusammenfassung der Projektdokumentation bis 30. September 2023.

4.1.3 Resümee des Projekts „ALARM Informationssicherheit“ auf Englisch

Scholl, M. (2024c). Résumé of the Gamified Increase in Security Awareness in German Small and Medium-Sized Businesses after Three Years’ Practice of “ALARM Information Security” doi:10.13140/RG.2.2.13519.29600.

Veröffentlicht als Preprint:



March 13, 2024 / DOI: 10.13140/RG.2.2.13519.29600 / License: CC BY 4.0

Résumé of the Gamified Increase in Security Awareness in German Small and Medium-Sized Businesses after Three Years’ Practice of “ALARM Information Security”

Margit C. Scholl
University of Applied Sciences Wildau (TH Wildau)
Hochschulring 1, 15745 Wildau, Germany
margit.scholl@th-wildau.de

Abstract

Latest cybersecurity reports for 2023 again show a critical situation in IT security in Germany—in fact, the threat in cyberspace is higher than ever before. There can be no doubt that small and medium-sized enterprises (SMEs) need to build their cyber resilience with people. Humans are increasingly becoming the center of events to increase information security. Within just three years and under the difficult conditions of the COVID-19 pandemic, the “Awareness Lab SME (ALARM) Information Security” project has developed a practice-oriented mix of methods in analog and digital form (serious games). All the tested materials have now been made available free of charge. The aim of the overall scenario was to promote the urgently needed operational awareness raising of executives and employees in SMEs. This article summarizes the key findings.

Keywords

Information security, awareness raising, serious games, awareness training, on-site attack simulations, low-threshold security concepts

Abbildung 24 Erste Seite der englischsprachigen Zusammenfassung des Projekts bis 31. März 2024.

4.2 Bericht der Abschlussevaluation

4.2.1 Resümee

Sowohl in der umfangreichen Projektdokumentation auf Deutsch (Scholl, 2024a) als auch im Resümee auf Englisch (Scholl, 2024c) werden die einzelnen Teilaspekte des Projekts „ALARM Informationssicherheit“ eingehend evaluiert und die gewonnen Erkenntnisse dokumentiert.

4.2.2 Gemeinsam zum Projekterfolg

Eine besondere Art der Evaluation stellt der Report 3 dar, der die beteiligten Akteure zu Wort kommen lässt (von Tippelskirch, Prott, & Scholl, 2023), wodurch der gemeinsam erreichte Projekterfolg dokumentiert wird.

Gemeinsam zum Projekterfolg

Mehr Einblicke in unserem Projektvideo!

alarm.wildau.biz

IMPRESSUM

Herausgeberin
Prof. Dr. Margit Scholl
Technische Hochschule Wildau
Hochschulring 1
15745 Wildau
alarm@th-wildau.de
Autor und Autorinnen
Hubertus v. Tippelskirch
Frauke Prott
Margit Scholl
Gestaltung
Olesja Mujkic und
Forschungsgruppe Scholl
Bilder
Falls nicht entsprechend mit Quellen anders vermerkt, Bildnachweis:
© Forschungsgruppe Scholl
Titelgrafik: Forschungsgruppe Scholl

September 2023

ISBN 978-3-949639-07-4

INHALT

Abbildung 25 Inhaltsverzeichnis des Reports 3 des Projekts „ALARM Informationssicherheit“ (Abschlussevaluation)

4.2.3 Video des Projekts als Abschlussevaluation

Nach der Projektabschlussveranstaltung „Awareness Forum“ im Juni 2023, also quasi „am Ende des Tages“ haben auch die beteiligten KMU deutlich ihre Anerkennung für das Projekt ausgesprochen und die Erfolgsgeschichten im Report 3 (s. Kapitel 4.2.2) bezeugen die großartige Leistung des Forschungsteams und der Unterauftragnehmenden im Projekt.

Mehr noch: Sowohl von beteiligten wie auch externen KMU wurde der Wunsch geäußert, in einem neuen Projekt mit einer durchaus dominanten Rolle als Industrie- oder Dienstleistungspartner beteiligt zu werden. Aktuell verbliebene Notwendigkeiten waren bereits von der Projektleiterin, Prof. Scholl, beim BMWK als neues Fokusprojekt eingereicht; dieses wurde jedoch nicht bei der Auswahl für eine neue Förderung vorgesehen. Das Forschungsteam musste und muss sich zu anderen Arbeitsmöglichkeiten umorientieren.

Das Forschungsteam der TH Wildau hat ein Video auf Deutsch mit beteiligten Pilotunternehmen und Nutzenden als Abschlussevaluation produzieren lassen. Dieses enthält eine zusammenfassende Veranschaulichung, Reflexion und Abschlussevaluation des Projekts „ALARM Informationssicherheit“ (s. Abb. 11).

4.2.4 Fünf aktuelle Podcasts zu den Projektergebnissen zur internationalen Bekanntmachung und Evaluationsbilanz

Unser Pionierprojekt „ALARM Informationssicherheit“ mit einem intelligenten Methoden-Mix stieß in Deutschland bereits während seiner ursprünglichen Laufzeit auf große Resonanz. Dies zeigen auch unsere nachgefragten Aktivitäten in der KNV.

Daher wurden in der KNV anhand der aktuellen englisch-sprachigen Veröffentlichungen auch fünf entsprechende Podcasts für den internationalen Markt konzipiert und durch Research Publishing International Ltd veröffentlicht, inklusive Social Media und Video Promotion über die nächsten vier Monate.

Dies dient der internationalen Bekanntmachung des deutschen Projekts „ALARM Informationssicherheit“, denn deutsche KMU agieren zunehmend international, haben Mitarbeitende internationaler Herkunft und Englisch als vereinheitliche Sprache, so dass diesem Umstand entsprochen werden muss. Dies wird auch im nachfolgenden Erfahrungsbericht der IHK Ostbrandenburg deutlich, denn deutsche KMU mit vielen ausländischen Mitarbeitenden wünschen sich die entwickelten Serious Games des Projekts „ALARM Informationssicherheit“ auch auf Englisch.

Obwohl sich das Projekt und seine hochwertigen Materialien an deutsche Unternehmen richtet, wird es nicht nur von anderen deutschen Institutionen geschätzt, sondern es hat nicht zuletzt aufgrund seines neuen Ansatzes in der Informationssicherheitssensibilisierung zudem eine deutliche internationaler Relevanz. Die Podcasts werden ab 26. März 2024 sukzessive freigeschaltet.

Link: https:// researchpod.org/informatics-technology

1. Podcast, 26.3.2024: https://researchpod.org/informatics-technology/security-sensitization

Die genauen Links pro Podcast werden auch der Projektwebseite unter „Presse“ zu entnehmen sein.

4.2.5 Erfahrungsbericht der IHK Ostbrandenburg zur Nutzung des „Awareness-Koffers“ in der KNV des Projekts

IHK Ostbrandenburg

Erfahrungsbericht Projekt Alarm – Nutzung des IT-Sicherheitskoffers September 2023 - Februar 2024

Im Projekt ALARM, dem Awareness Labor KMU für mehr Informationssicherheit, der TH Wildau wurden sieben analoge serious Games entwickelt. Diese IT-Sicherheitsspiele sind qualitativ sehr hochwertig und in einem Reisekoffer verpackt. In der Praxis kamen die Spiele Homeoffice, Multi-Faktor-Authentifizierung, Mobile Apps und Daten- & Informationsschutz bei den bisherigen Teilnehmern besonders gut an. Die Spiele zu den Themen CEO Fraud, Social Engineering und Infoklassen-Roulette wurden im Moment noch nicht nachgefragt.

In den folgenden Darstellungen werden die Aktivitäten mit dem Koffer detaillierter beschrieben und einige Hinweise für das Projekt gegeben.

Nach Erhalt des IT-Sicherheitskoffers gab es vier Vorstellungsrunden bei den Partnern IHK-Projektgesellschaft mbH im Zukunftszentrum Brandenburg, beim Mittelstand-Digital Zentrum Spreeland in Eberswalde, beim IHP Leibniz-Institut für innovative Mikroelektronik Frankfurt (Oder) und bei den IT Administratoren der IHK Ostbrandenburg. Alle Vorstellungsrunden endeten mit dem Versprechen weitere Schulungsaktivitäten in den Monaten November 23 – Februar 24 zu entwickeln. Die IT Administratoren waren gleich so engagiert, dass sie alle sieben spiele hintereinanderweg durchprobierten und den Innovationstag der IHK als mögliche Mitarbeiterschulung vorschlugen. Danach erfolgte eine vertiefte Einarbeitung von vier Mitarbeitern durch die Spielleitfäden.

Die Spiele HomeOffice und Multi-Faktor-Authentifizierung wurden am **17.10.** in der **Dienstberatung der Abteilung Wirtschaftspolitik** mit 14 Kolleginnen und Kollegen ausprobiert. Es zeigte sich, dass bei beiden Themen bereits ein hoher Kenntnisstand vorhanden war und im HomeOffice-Bereich keine Fehler gemacht wurden. Bei der richtigen Zuordnung der Passwörter wurden bezüglich der Komplexität und Länge von Passwörtern Lerneffekte erzielt. Beim HomeOffice-Spiel wünschten sich zwei Kolleginnen eine Gesamtübersicht der Spielkarten, um auch die anderen Inhalte, die nicht selbst gelegt wurden, zum späteren Nachlesen für sich selbst zu erschließen. Dieser Test im kleineren Kollegenkreis bestärkte den Einsatz beim **IHK Innovationstag am 8.12.2023.**

In der Einführung des Innovationstages wurden alle Teilnehmer auf die interaktive Methodik der serious Games vorbereitet und auf die digitalen Games als Ergänzung hingewiesen. In sechs Gruppen a 8-10 Mitarbeitern wurden die Spiele Homeoffice,

IHK Ostbrandenburg | Puschkinstraße 12 b | 15236 Frankfurt (Oder)
Tel.: 0335 5621-0 | Fax 0335 5621-1196 | info@ihk-ostbrandenburg.de | www.ihk.de/ostbrandenburg

IHK-Erfahrungsbericht, Fortsetzung:

Multi-Faktor-Authentifizierung, Mobile Apps und Daten- & Informationsschutz an Tischinseln gespielt. Alle Mitarbeiter nahmen engagiert teil und gaben positive Rückmeldungen zu den Lernerlebnissen. Insbesondere zum Thema HomeOffice wurden Erfahrungen von zu Hause ausgetauscht und einige Problembereiche oder Wissenslücken erkannt. Durch das spielerische Herangehen verspürten die Mitarbeiter keinen Druck etwas falsch zu machen. Einige Mitarbeiter packte der Ehrgeiz und wollten nach den Runden noch weiterspielen.

Die IHK führte in den Monaten Januar und Februar noch zwei weitere Mitarbeiterschulungen mit Themen der Informationssicherheit über ein Online-Schulungsportal durch. Die Spiele des Alarmprojektes halfen hier sicherlich für ein besseres Verständnis und einer höheren Teilnahme.

In den kommenden Wochen soll der Koffer noch im Beraternetzwerk der IHK Ostbrandenburg zum Einsatz kommen.

Beim IHP wurde bisher bei den ca 350 Mitarbeitern noch kein Termin gefunden. Der zuständige Mitarbeiter informierte darüber, dass es ein hohes Sicherheitsempfinden bei allen Mitarbeitern gäbe und fragte nach einer englischen Version, da hier sehr viele ausländische Mitarbeiter tätig sind. Der Einsatz des Koffers ist im Gedächtnis und wird, wenn es passt noch erfolgen.

Im Rahmen des Zukunftszentrum Brandenburg konnte die IHK Projektgesellschaft **einen Inhouse-Workshop am 20.12.2023** im Unternehmen **WELTEC Produktion** Wollup GmbH in Letschin durchführen. Hier wurden die Games von Multi-Faktor-Authentifizierung und Daten- & Informationsschutz mit 12 Mitarbeitern des Unternehmens gespielt.
Der IT Sicherheitskoffer ist ins Beratungsangebot des Zukunftszentrums aufgenommen.

Seit Januar 2024 befindet sich der Koffer im Mittelstand-Digital Zentrum Spreeland in Eberswalde und ein Mitarbeiter arbeitete sich in die Spiele ein. Ein Angebot zum Thema IT Sicherheit ist aufgrund anderer Themen noch nicht bis Ende Februar erfolgt. https://www.digitalzentrum-spreeland.de/Veranstaltungsarchiv. Ein Interesse im 2. HJ 2024 besteht.

Abbildung 26 Erfahrungsbericht der IHK Ostbrandenburg, ein sehr aktiver Partner im Projekt, der den „Awareness-Koffer" mit den analogen Serious Games umfangreich und auch weiterhin nutzt.

4.2.6 Evaluationsbeteiligung

Am 3. November 2023 hatte Sustainable Society Transformation / Ramboll Management Consulting GmbH ein einstündiges Interview mit Prof. Scholl als Projektleiterin angefragt, das der Evaluation der BMWK-Initiative „IT-Sicherheit in der Wirtschaft“ dienen soll. Das Interview wurde am 29. November 2023 durchgeführt. Im Nachgang wurde eine kurze Online-Befragung für KMU im Januar 2024 angekündigt. Die Unterauftragnehmenden und die Pilot-KMU wurden darüber informiert und der Link wurde nach Rücksprache weitergeleitet. Ein Ergebnis ist der TH Wildau bislang nicht bekannt.

Abschluss-Bild des Projekts „ALARM Informationssicherheit“:

Abbildung 27 Abschließendes Ergebnisbild für den Schlussbericht.

Abschluss-Cover des Schlussberichts „ALARM Informationssicherheit“:

Abbildung 28 Abschließender Buchumschlag für den Schlussbericht.

Projektwebseite: https://alarm.wildau.biz

Technische Hochschule Wildau
Technical University of Applied Sciences

WILDAU

Unterauftragnehmer des Projekts

gamebook

known_sense
awareness you can touch.

sudile
supported distance learning

Thinking Objects

Weitere Informationen zum Projekt
https://alarm.wildau.biz/

Awareness Labor KMU (ALARM) Informationssicherheit hat in enger Zusammenarbeit mit der Praxis effektive Lösungen für Sensibilisierung und Qualifizierung in kleinen und mittleren Unternehmen (KMU) zur Steigerung des Informationssicherheitsbewusstseins geschaffen:

Analoge Serious Games mit Anleitungen sowie niederschwellige Sicherheitskonzepte für KMU mit Informationsblättern stehen für eine interne, nicht-kommerzielle Sensibilisierungsmaßnahme zum Download bereit. Digitale Serious Games und ein Selbsttest können unter gleichen Bedingungen direkt über die Projektwebseite durchgeführt werden. Weitere Ergänzungen zu Veranstaltungen, Flyer, Poster, Broschüren und wissenschaftliche Artikel können genutzt werden.

ISBN 978-3-949639-09-8
9 783949 639098

Projektlaufzeit: 01.10.2020–31.03.2024

Wildau: TH Wildau