ALARM
Awareness Labor KMU
Informationssicherheit

Game over vs. Game Lover

Serious Games als wirksame Security Awareness-Maßnahmen für KMU im Projekt »ALARM Informationssicherheit« – Framework mit Kommunikationsleitfaden, FAQ und Ausblick

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Impressum

Herausgeberin und Kontakt

Prof. Dr. Margit Scholl
Technische Hochschule Wildau
Hochschulring 1
15745 Wildau
alarm@th-wildau.de

Das vorliegende Dokument ist die dritte und letzte Studie des Projektpartners und Unterauftragnehmers known_sense im Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ nach

- Qualitative Wirkungsanalyse Security Awareness in KMU. Tiefenpsychologische Grundlagenstudie im Projekt „ALARM Informationssicherheit“
- Enabling vs. Entmündigung. Qualitativer Konzepttest analoger Security Awareness-Lernszenarien für KMU im Projekt

https://alarm.wildau.biz/

Grundlage dieser Studie ist Desk Research, u. a. mit den beiden oben benannten tiefenpsychologischen Wirkungsanalysen, u. a. basierend auf Tests, Fokusinterviews bzw. Gruppendiskussionen mit insgesamt 136 Probanden/-innen aus KMU. Darüber hinaus kamen insbesondere auch beim FAQ und den Detailempfehlungen die Erfahrung während dieses Projektes und die 20-jährige Erfahrung von known_sense in Bezug auf Security Awareness-Kampagnen bei mehr als 150 Organisationen bzw. Unternehmen sowie insbesondere bei der Kreation und Durchführung von Lernstationsformaten (u. a. Serious Games) bzw. der Erstellung interner Security Awareness-Konzepte und -Frameworks für Kunden/-innen zum Zuge

Das Projekt wird vom Bundesministerium für
Wirtschaft und Klimaschutz (BMWK) in der Initiative IT-Sicherheit in der Wirtschaft im Förderschwerpunkt „Mittelstand-Digital“ gefördert.

Projektlaufzeit

01.10.2020 – 31.03.2024

Der Leitfaden wurde von known_sense von Juni bis August 2023 zusammengefasst und mit dem Forschungsteam Scholl der TH Wildau beraten.

Das BMWK hat die Veröffentlichung im August 2023 freigegeben.

Das in diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des (BMWK) unter dem Förderkennzeichen 01MS19002A gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren/-innen.

Verantwortlich für Inhalt und Gestaltung:

known_sense | Jakob-Engels-Str. 39 | 51143 Köln

Autoren:

Dietmar Pokoyski |
Dipl.-Psychologin Ankha Haucke | Prof. Margit Scholl

Abbildungen:

Abbildungen Forschungsteam „Information Security Awareness”
Prof. Margit Scholl an der TH Wildau außer Coverfoto (shutterstock)
und Abb. 4 bis 9 (known_sense)

August 2023

ISBN 978-3-949639-08-1

Game over vs. Game Lover

Serious Games als wirksame Security Awareness-Maßnahmen
für KMU im Projekt »ALARM Informationssicherheit«
– Framework mit Kommunikationsleitfaden, FAQ und Ausblick

Inhaltsverzeichnis

Auoren/-innen

- Dipl. Psychologin Ankha Haucke und Dietmar Pokoyski, known_sense: Vorwort und Kapitel 1 bis 4
- Prof. Dr. rer. nat. Margit C. Scholl, TH Wildau: Kapitel 5

Abb. 1: *Test des analogen Serious Game „ultifaktor-Authentifizierung (Kap. 3.3.2) durch die TH Wildau*

Vorwort

Unternehmen werden seit jeher, d. h. seit Beginn betriebswirtschaftlichen Handelns, angegriffen, betrogen und bestohlen. Während jedoch klassische, analoge Wirtschaftsdelikte abnehmen, steigen die digitalen mit ungebremster Vehemenz an. All das, was uns technologischen Fortschritt bringt, kann auch für Straftaten ausgenutzt werden. Im Mix mit traditionellen Betrugsmaschen oder psychologisch intendierten Manipulationen, wie z. B. Social Engineering, entsteht eine kaum noch kontrollierbare Cyber-Streumunition, die Wirtschaft und Bürger/-innen unter Dauerbeschuss nimmt.

So ist, laut der Studie „Wirtschaftsschutz 2022“, herausgegeben von Digitalverband Bitkom [1], bei den analogen Delikten z. B. der Diebstahl physischer Dokumente mit 42 Prozent um 8 Prozentpunkte gegenüber dem Vorjahr zurückgegangen. Ähnlich verhält es sich mit dem Abhören von Besprechungen – face-to-face oder per Telefon – (28 Prozent, minus 9 Prozentpunkte) und mit so genannter analoger Sabotage (22 Prozent, minus 3 Prozentpunkte). Demgegenüber geben in derselben Studie mit 69 Prozent mehr als zwei Drittel der Unternehmen an, dass sie in den vergangenen zwölf Monaten von Diebstählen ihrer IT- und Telekommunikationsgeräte betroffen oder vermeintlich betroffen waren. Dieser Wert stellt einen Anstieg um 7 Prozentpunkte zum Vorjahr dar. Knapp zwei Drittel, d. h. 63 Prozent, konnten einen Diebstahl sensibler Daten verzeichnen – ein Anstieg von 3 Prozentpunkten gegenüber dem Vorjahr. Bei 57 Prozent der Unternehmen wurde digitale Kommunikation ausgespäht – ein Anstieg von 5 Prozentpunkten. Und 55 Prozent waren tatsächlich oder gefühlt von digitaler Sabotage ihrer IT- Systeme oder anderer wichtiger Prozesse betroffen oder vermuten dies zumindest (plus 3 Prozentpunkte).

Beim Diebstahl digitaler Daten haben es die Angreifer heute offenbar vor allem auf Daten Dritter abgesehen. So geben 68 Prozent der vom digitalen Diebstahl betroffenen Unternehmen an, dass Kommunikationsdaten wie E-Mails (plus 5 Prozentpunkte gegenüber dem Vorjahr) oder etwa Cloud-Zugangsdaten (32 Prozent) entwendet wurden. Bei einem Viertel (25 Prozent) waren Daten eigener Mitarbeiter/-innen und bei fast der Hälfte (45 Prozent) auch Kundendaten betroffen (plus 14 Prozentpunkte). Diese Aspekte sind insofern stark zu gewichten, da beim Verlust von Daten Dritter den Unternehmen enorme Kollateralschäden durch Bußgelder oder Reputationsverluste drohen.

Vor allem Betreiber kritischer Infrastrukturen (KRITIS) sind vom Anstieg in Bezug auf Cyberangriffe besonders stark betroffen. Bei 87 Prozent der KRITIS-Unternehmen haben Cyberattacken zugenommen. So ist es auch kein Wunder, dass die Sorgen vor den Folgen eines derartigen Angriffs weiter anwachsen: Unternehmen erwarten in den kommenden zwölf Monaten in jedem Fall eine weitere Zunahme von Cyberangriffen, vor allem infolge von Ransomware. 78 Prozent der Unternehmen rechnen mit einem starken oder sehr starken Anstieg bei Erpressungstrojanern. Beinahe die Hälfte der Unternehmen (45 Prozent) sind in Bezug auf ihre geschäftliche Existenz beunruhigt – mit plus 36 Prozentpunkten ein deutlicher Anstieg gegenüber dem Vorjahr.

Kein Wunder – Unternehmen in Deutschland hatten seit Beginn der Corona-Pandemie die Digitalisierung mit Hochdruck vorangetrieben und lassen auch heute noch deutlich mehr Mitarbeiter/-innen in Home Offices außerhalb ihrer angestammten IT-Infrastruktur arbeiten. Angriffe auf Unternehmen haben sich zuletzt nicht nur deswegen zunehmend in den digitalen Raum verlagert. Bei den Angriffsvektoren liegen Passwortattacken, Phishing, Malware, Ransomware, DDoS-Attacken und Social Engineering vorne. Beinahe die Hälfte der Unternehmen (48 Prozent) war von Social Engineering betroffen.

Gerade diese zunehmende Anzahl von Angriffen auf Menschen mithilfe sozialer Manipulation, der technisch nicht beizukommen ist, oder aber Multivektorangriffe, bei denen Social Engineering mit technischen Vektoren kombiniert wird, beunruhigen die Wirtschaft immens. Achim Berg, Präsident des Bitkom e. V., stellt dazu fest: „Eine regelmäßige Schulung von Mitarbeiter/-innen zu Sicherheitsfragen, damit sie sich auch bei Social-Engineering-Versuchen richtig verhalten, sollte in jedem Unternehmen selbstverständlich sein.“ Und „bei den Ausgaben für IT-Sicherheit müssen die Unternehmen dringend zulegen. Die Erkenntnis, welche dramatischen Folgen ein erfolgreicher Angriff haben kann, ist längst da – den notwendigen Schutz davor gibt es aber nicht zum Nulltarif. Hier müssen Vorstände und Geschäftsleitungen umgehend aktiv werden“, sagt Berg [2].

Mit der hier verwendeten, eher traditionellen Bezeichnung „Schulungen“ sind vermutlich Security Awareness-Maßnahmen gemeint, die allerdings nicht nachhaltig geraten, wenn der Fokus tatsächlich traditionell ausschließlich auf Lerntheorie und Wissensvermittlung gelegt wird, so wie es die Bezeichnung „Schulung“ impliziert. Zudem erfordert die Entwicklung bei den Angriffsvektoren auch bei der Abwehr nicht ausschließlich reines Wissen um Funktionsweisen von Dingen bzw. Prozessen, sondern zunehmend Verständnis für die paradoxen Verhältnisse menschlicher Kommunikation und sozialer Beziehungen. In diesem Kontext sind reine Schulungen oder klassische Trainings mit der Vermittlung von Regeln, Compliance und Informationshäppchen nicht mehr ausreichend, um das Niveau an Awareness zu adressieren, das angesichts zunehmender und komplexer werdender Cyberattacken benötigt wird.

Abb. 2: *Test des analogen Serious Game „Infoklassen-Roulette“ (Kap. 3.3.6) durch die TH Wildau*

Zu den Präventionsmaßnahmen bei Cyberkriminalität zählen neben Awareness-Maßnahmen im weitesten Sinne auch Cyberversicherungen, die vorgeben, Schäden bei möglichen Incidents zu regulieren. Diese sind wiederum auch Treiber von Awareness (s. Kapitel 2.2). Neben der Bitkom und einigen anderen Organisationen verwundert es daher nicht, dass auch Finanzdienstleistungsunternehmen wie z. B. die Gothaer Versicherung, die im Bereich der Cyberkriminalität – wie auch die meisten anderen Versicherungen – längst neue Geschäftsfelder erschlossen hat, als Absender von Security-Studien auftritt. Und mehr noch – die Gothaer KMU-Studie nimmt sogar die Zielgruppe der hiesigen Initiative „ALARM Informationssicherheit“ unter die Lupe und stellt fest, dass vom Anstieg der Cyberkriminalität eben auch KMU betroffen sind. Auf Platz Eins der Bedrohungen liegt nach dieser Studie die Befürchtung, Opfer eines Hackerangriffs zu werden (48 Prozent). Auch im KMU-Umfeld wird betont, dass in den letzten fünf Jahren das Bewusstsein für das Risiko, Opfer von Cyberkriminalität zu werden, kontinuierlich gestiegen ist (48 Prozent 2022 gegenüber 32 Prozent 2021), während auch hier immer weniger die Risiken analoger Delikte wie z. B. Einbrüche (30 Prozent) befürchtet werden [3].

Auch Anbieter/-innen anderer Versicherungen wie etwa die Munich Re gehen davon aus, dass sich der Markt für Cyberpolicen in den nächsten zwei Jahren aufgrund der ansteigenden Zahl von Cyberattacken mindestens verdoppeln wird. 2022 feierte die Branche einen Rekordumsatz in Höhe von circa 12 Milliarden US-Dollar [4]. Dabei geht die Munich Re in ihrem Report „Cyber Insurance: Risks and Trends 2023” vor allem von Ransomware als Hauptursache für Schäden in den Unternehmen aus [4] [5].

Das Internet Crime Complaint Center (IC3) des FBI bezifferte die Verluste durch Ransomware im vergangenen Jahr auf 29,1 Millionen US-Dollar. Dabei ist bei dieser Schätzung davon auszugehen, dass sie nur einen Bruchteil der Schäden abdeckt, die von Unternehmen aus verschiedenen Gründen verschleiert oder gar nicht kommuniziert werden. Ein Bericht des Magazins Cybersecurity Ventures prognostiziert, dass Ransomware den betroffenen Unternehmen bis 2031 jährlich rund 265 Milliarden US-Dollar kosten wird, wobei alle zwei Sekunden ein neuer Angriff stattfindet [6]. Eine Hochrechnung aus den bereits abgeschlossenen Cyberversicherungen, den für die kommenden Jahre berechneten Werten und aktuellen Schadensmeldungen zeigt jedoch, dass das Marktpotential von Cyberpolicen deutlich über der Schätzung von Cybersecurity Ventures liegen dürfte [4].

Ob eine Schadensdelegation an Cyberversicherungen ausreichend ist, um künftige Risiken bzw. Schäden zu minimieren, darf zurecht bezweifelt werden. Denn die Forderung nach dem Nachweis von z. B. Awareness-Maßnahmen ist den meisten dieser Versicherungen bereits inhärent. Das heißt, selbst die Versicherungen gehen davon aus, dass potenziell zu regulierende Schäden infolge der Sensibilisierung von Mitarbeiter/-innen der Versicherungsnehmer/-innen begrenzt werden können.

Gerade die sich zuletzt abzeichnenden Trends mit Double Extortion, Veröffentlichung bzw. Verkauf sensibler Daten – auch Dritter – im Dark bzw. Deep Web oder Angriffe zur Unterbrechung der seit der Corona-Pandemie sensiblen Lieferketten zeigen, dass sich im digitalen Raum längst mafiöse Strukturen etabliert haben und sich das Abkassieren von Erpressungs- und Schutzgeldern bei geringer Aufklärungsquote als ein sehr lohnendes Geschäftsmodell etabliert hat. Darüber hinaus tragen Entwicklungen wie „Rent a Hacker“, RAAS (Ransomware as a Service) und nicht zuletzt KI (Künstliche Intelligenz) dazu bei, cyberkriminelle Handlungen zu professionalisieren, einfacher und preisgünstiger zu gestalten bzw. weiter zu verbreiten.

Gerade KI kann dazu beitragen, Cyberkriminelle noch unabhängiger von Expertenwissen um IT im Allgemeinen und Skripting im Besonderen zu machen – just zu einem Zeitpunkt, als die Defense-Seite ihre Tools, die auch mithilfe von KI in Bezug auf die Abwehr agieren, glaubte ihre Systeme in trockene (Schutz-)Tücher gebracht zu haben. Wir sehen: der ewige Wettlauf um Digitalisierung im Cyberraum ist eine „never ending story“. Jede technische Entwicklung, die der Abwehr nützt, kann auch zum Angriff missbraucht werden. Wenn es am Ende zu einer technischen Pattsituation kommt, ist es der Mensch, der im „Elfmeterschießen“ um den Cyberraum die „richtige“ Entscheidung treffen muss. Das ist eine gute Nachricht für die Security Awareness – es geht nicht ohne sie und – kognitiv, aber auch intuitiv – nicht ohne die Menschen an ihren Arbeitsplätzen.

Abb. 3: *Test des analogen Serious Game „Infoklassen-Roulette“ (Kap. 3.3.6) durch die TH Wildau*

1.Einleitung

In diesem Dokument geht es um Security Awareness und wie diese vorrangig in kleinen und mittleren Unternehmen (KMU) umgesetzt wird. Damit bildet diese dritte Studie als Teil des Abschlusses des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“ eine Art Security Awareness-Framework mit möglichen konzeptuellen und praktischen Grundlagen für alle Awareness-Maßnahmen bzw. -Kampagnen in KMU. Der vorliegende Leitfaden soll als praktischer Ratgeber zur Selbsthilfe Multiplikatoren/-innen von Security Awareness, Geschäftsführenden, IT- bzw. Sicherheitsexperten/-innen dabei unterstützen, Awareness-Maßnahmen zu Informationssicherheits- und Datenschutzthemen zu planen, durchzuführen und zu evaluieren.

Der inhaltliche Schwerpunkt liegt auf den im Projekt „ALARM Informationssicherheit“ entwickelten teambasierten, analogen Serious Games, da diese – anders als z. B. die parallel entwickelten geschlossenen Single Player-Varianten der digitalen Serious Games äußerst flexibel – mithin individuell – einsetzbar sind und durch Anlass, Dauer, Schwerpunkt-Ausrichtung, Moderation, skalierbare Zielgruppen-Affinität bzw. Verknüpfung mit anderen Maßnahmen deutlich mehr Begleitung erfordern als „fertige“ digitale Games oder etwa andere E-Learning-Tools der zahlreichen, oft verwechselbaren Plattform-Awareness-Anbieter/-innen

Security Awareness muss nach Normen bzw. Gesetzen ein fester Bestandteil der Geschäftsabläufe auf allen Ebenen aller Organisationen sein. Es existiert jedoch quer durch alle Organisationen ein unterschiedliches Verständnis davon, was Security Awareness bedeutet. Je nach Zuschreibung von der klassischen Lerntheorie bis zu neuesten Change-Ansätzen umfasst Awareness verschiedene Methoden (s. Kapitel 2.3) und Instrumente (s. Kapitel 2.3.4). Inhalte und Ausführung hängen daher u. a. vom Verständnis dieser Methoden, Geschäftsmodell, Unternehmens- und Sicherheitskultur (s. Kapitel 2.1.2), Größe, Zeitressourcen, Budgets und mehr ab.

Die hier dargestellten Methoden bzw. Instrumente berücksichtigen

- die Sicherheitskultur von Organisationen,
- den Reifegrad der Organisationen
- und den Wissenstand bzw. die Reife der Beschäftigten.

In Kapitel 2, dem theoretischen Abriss dieses Leitfadens, werden Awareness-Treiber und methodische Grundlagen der Security Awareness in Form eines Frameworks dargestellt. In Kapitel 3 werden die im Rahmen des Projektes „ALARM Informationssicherheit“ entwickelten Formate, je 7 analoge und digitale Serious Games, vorgestellt und in einen Kontext zueinander und zu anderen möglichen Sensibilisierungsinstrumenten gesetzt. In Kapitel 4, dem ganz praktischen Teil, stellt ein FAQ Fragen und Antworten im Kontext der analogen Serious Games vor, vor allem hinsichtlich Planung, Ausführung, Moderation und Dokumentation von verdichteten Trainingsevents mithilfe synchron durchgeführter, analoger Serious Games und mehr als 60 Teilnehmenden. Das Kapitel 5 kumuliert Erkenntnisse aus dem Gesamtszenario und den drei Studien des Projekts „Awareness Labor KMU (ALARM) aus Sicht der Herausgeberin.

1.1 Das Projekt „ALARM Informationssicherheit“

Kleinst- bis mittlere Unternehmen (KKU bzw. KMU) erheben, verarbeiten und nutzen viele sensible Daten mit Hilfe von digitalen IT-Lösungen, unterschätzen jedoch häufig die Risiken und Bedrohungslage durch immer raffinierter agierende Angreifende. Sorglosigkeit über Informationssicherheit sowie Unkenntnis oder Verletzung von betrieblichen Richtlinien oder nichtexistierende Informationssicherheitsrichtlinien sind Risiken für Unternehmen aller Art und Größe. Die vielfältigen Schwachstellen stellen Sicherheitsmängel dar, die zukünftige verzögerte Folgen für KMU/KKU haben können. Hier setzt das multidisziplinäre Forschungsprojekt „ALARM Informationssicherheit“ an.

Das Projekt hat von 2020 bis 2023 ein Gesamtszenario zur Sensibilisierung und Unterstützung der KKU/KMU für Informationssicherheit bis hin zu deren Selbsthilfe aufgebaut. Im Projekt wurde 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 entwickelt. Das Gesamtszenario soll zu der dringend notwendigen Sensibilisierung von Führungskräften und Mitarbeiter/-innen und zu einer gezielten Personalentwicklung in KMU/KKU führen, wie sie derzeit breitenwirksam noch nicht vorhanden ist. Dazu wird IT-Sicherheit in Zusammenhang mit den zunehmend digitalen Arbeitsprozessen konkret (be-)greifbar gemacht, gleichzeitig werden die Menschen emotional berührt und aktiv in die Entwicklung von Maßnahmen einbezogen. Eine nachhaltige und unternehmensweite Informationssicherheitskultur soll damit aufgebaut werden.

Es werden Defizitbereiche wichtiger Geschäftsprozesse systematisch und gemeinsam mit Pilot-KMU und -Handwerksbetrieben anhand konkreter Tätigkeiten erschlossen und Sicherheits- sowie Kompetenzprofile abgeleitet. Um Nachhaltigkeit auch breitenwirksam zu erreichen, werden aktivierende Sensibilisierungsmaßnahmen analog

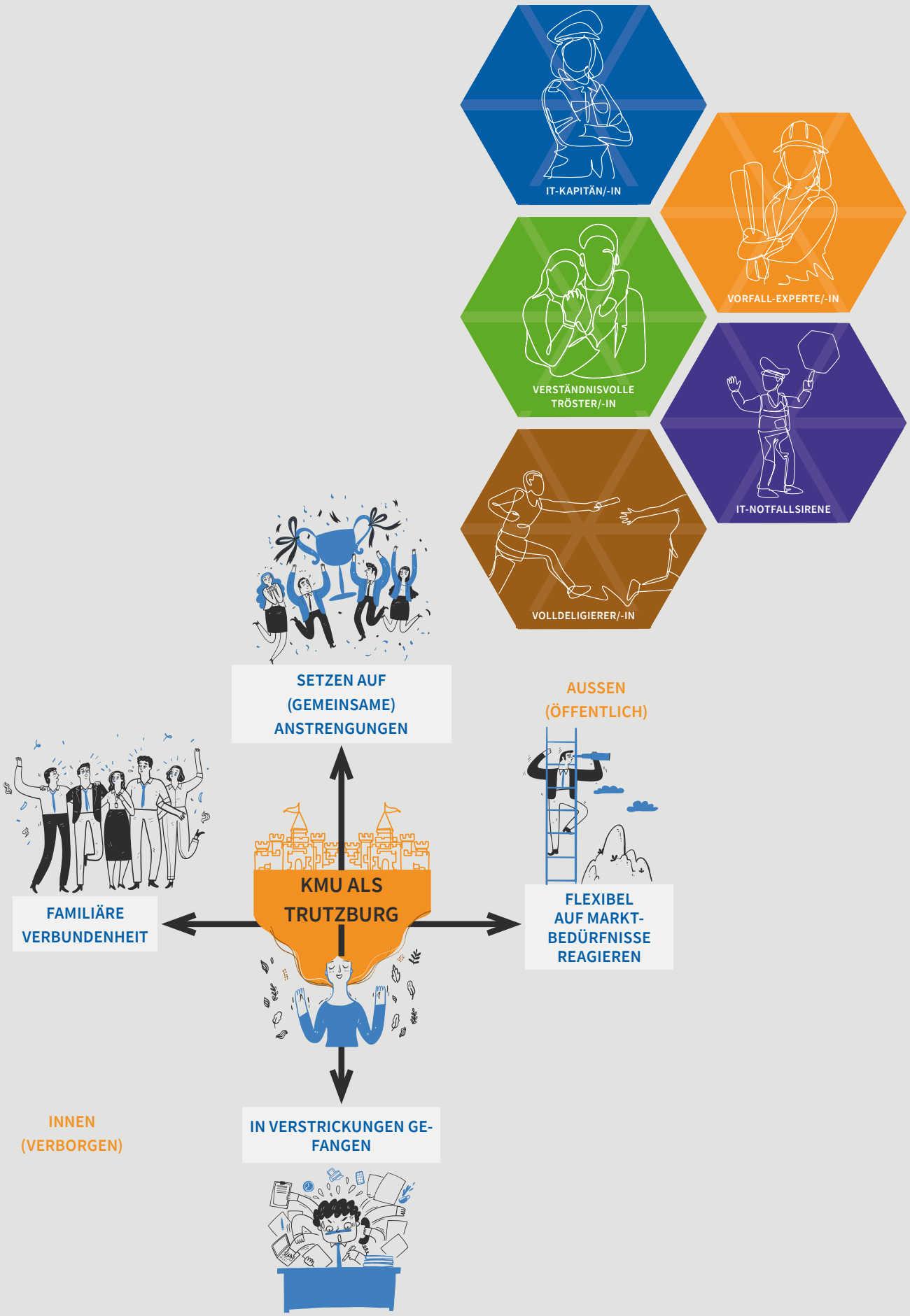


Abb. 4 und 5: *Psychologische Konstruktion der Sicherheitskultur in KMU (oben rechts) und Typologie Security-Multiplikatorinnen und Multiplikatoren (unten links) aus der KMU-Grundlagenstudie [11]*

und digital entwickelt, praktisch vielfältig erprobt und evaluiert. Best-Practice-Anleitungen mit Erfolgsgeschichten teilnehmender Unternehmen werden bundesweit über assoziierte Transferpartner/-innen veröffentlicht, um weitere Unternehmen anzusprechen. Neuartige betriebliche Awareness-Messungen führen zu Reifegradaussagen für KMU/KKU. Qualitäts- und Ergebnissicherung, kombiniert mit Risikomanagement und einer begleitenden Evaluation, komplementieren die Wirkungsanalysen.

Zur Erreichung der Projektziele werden spezifische und auf die jeweiligen Bedürfnisse abgestimmte Schulungs- und Sensibilisierungskonzepte sowie Lernmaterialien entwickelt, getestet und evaluiert. Als Lernansätze hierfür werden Game-based und Accelerated Learning der Übertragung auf erlebnisorientierte Serious Games im Bereich Informationssicherheit zugrunde gelegt. Nach bisherigen Studien und Forschungsarbeiten von Prof. Dr. Scholl und des Forschungspartners known_sense erwiesen sich sowohl Emotionalisierung wie auch Motivation als essenziell für Lernprozesse in der Informationssicherheit. Alle entwickelten Materialien werden kostenlos allen Unternehmen per Download zur Verfügung gestellt, so dass bundesweit eine Verbesserung der Awareness und die Erhöhung des IT-Sicherheitsniveaus in Deutschland erreicht werden [7].

1.2 Sonderrolle KMU

Laut Definition der EU-Kommission fallen Unternehmen unter die Bezeichnung KMU (kleine und mittlere Unternehmen), wenn sie maximal 249 Mitarbeiter/-innen beschäftigen, einen jährlichen Umsatz von höchstens 50 Millionen Euro erwirtschaften bzw. über eine Bilanzsumme von höchstens 43 Millionen Euro verfügen [8].KMU gelten als Wirtschaftstreiber, weil die Einrichtung neuer Arbeitsplätze vorwiegend auf Unternehmen dieser Größenordnung zurückgeht [9]. KMU erheben, verarbeiten, übertragen und nutzen zahlreiche sensible Daten mithilfe digitaler Lösungen. Dabei wird ihnen jedoch allzu häufig eine gewisse Sorglosigkeit in Bezug auf Datenschutz, Informationssicherheit, Unkenntnis bzw. Verletzung von betrieblichen Richtlinien sowie nichtexistente bzw. lückenhafte Sicherheitsrichtlinien zugeschrieben, die eine Risikoerhöhung zur Folge hat. Die vielfältigen Schwachstellen sind Sicherheitsmängeln gleichzusetzen, die zukünftige verzögerte Folgen für KMU sowie KKU (Kleinst- und Kleinunternehmen) haben können. „Wenn wir einmal in ein Netzwerk eingedrungen waren, konnten wir dort machen, was wir wollten – wir waren praktisch wie Gott in den IT-Systemen“, sagt der White-Hat-Hacker Michael Wiesner in dem Report „Cyberrisiken im produzierenden Gewerbe“ [10]. Denn auch in KMU gilt genauso wie in Großunternehmen: Der Mensch ist und bleibt die größte Schwachstelle der Informationssicherheit und ist gleichzeitig deren größte Chance [10] hinsichtlich einer Resilienz im Sinne bewusst angewandter Abwehrmaßnahmen wie z. B. Security Awareness.

Generell unterscheiden sich die Cyberrisiken bei KMU nicht von denen der Konzerne bzw. Großunternehmen. Den Unterschied machen vor allem Unternehmens- bzw. Sicherheitskultur. Denn die hohe Identifikation und Verbundenheit mit zum Teil engen Bindungen und Produktionsstolz schaffen zwar Loyalität und bei der Führung ein hohes Vertrauen in die Mitarbeiter/-innen. Die Kehrseiten des harmonischen Miteinanders einer eher familiären Kultur wirken sich jedoch zum Teil kontraproduktiv auf die Informationssicherheit aus [11].

Der Anspruch an Security Awareness für kleinere Unternehmen – und gerade auch in Abgrenzung der vollmundigen Versprechen von Plattform-Awareness-Anbieter/-innen* – mag über diesen Leitfaden sehr ambitioniert formuliert sein. Da wir jedoch im Verlaufe des Projektes auf mittelständische Unternehmen getroffen sind, die verstanden haben, dass Security Awareness der vermutlich wichtigste Baustein im Kontext von Cyberangriffen darstellt und daher potenziell ihr Überleben sichert, können wir uns mit den Inhalten dieses Dokuments unmöglich auf den kleinsten gemeinsamen Nenner verständigen. Kleine Unternehmen und Kleinstunternehmen sind daher angehalten, sie in Bezug auf ihre Größe und Möglichkeiten unrealistisch erscheinenden Vorschläge und Tipps zu ignorieren und ausschließlich auf die Module zurückzugreifen, die ihnen sinnvoll erscheinen.

Wir wünschen allen KMU viel Erfolg bei der Neuausrichtung ihrer Sensibilisierungsaktivitäten.

Dipl. Psychologin Ankha Haucke und Dietmar Pokoyski, known_sense, Autoren/-innen Kapitel 1-4

Prof. Dr. rer. nat. Margit C. Scholl. TH Wildau, Herausgeberin und Autorin Kapitel 5

August 2023

**** Plattform-Awareness:** Hierunter verstehen wir die Delegation von Awareness-Programmen ausschließlich oder beinahe ausschließlich an Portale mit managed Services, also digitalen, vor allem lerntheoretisch ausgerichteten Inhalten ohne echten Rückkanal bzw. Möglichkeiten von beziehungsregulierenden Begegnungen und diskursiver Behandlung. Plattform-Awareness-Anbieter verheißen in der Regel Awareness-Erfolge ohne Aufwand („… mühelos …“) Sie können sie auch durch Werbewirkversprechen mithilfe von folgenden Schlagworten bzw. Slogans identifizieren, z. B. „… automatisierte Awareness …“, „… effektiv und kostengünstig …“, „… in wenigen Minuten aufsetzen …“, „KI-gesteuerte Kurse …“, „…mit kostenlosen Erweiterungen …“, „… einprägsamer Content …“, „… flexibler als jede Schulung vor Ort …“, „X00.000+ User …“ (Recherche „Security Awareness via Google am 28.07.2022, u. a. über die angezeigten Ergebnisse der Google Ads).*

Security Awareness im Sinne von Bewusstheit bedeutet, dass wir als Menschen bemerken, wenn eine Unterbrechung unserer Achtsamkeit in Bezug auf sicheres Verhalten stattfindet und wir gleichsam in der Lage sind, aktiv hierauf zu reagieren, indem wir unser „System“ so steuern, dass wir in der Lage sind, diese Aufmerksamkeit wiederherzustellen – oder wenn dies nicht gelingt – bewusst aus dieser Verfassung herauszutreten.

2. Security Awareness-Framework für KMU

Dieses Kapitel folgt inhaltlich im Wesentlichen dem von known_sense bei zahlreichen Großkunden/-innen eingeführtem Security Awareness Framework [12], wurde jedoch auf Basis der Projektanforderungen stark gekürzt und – auch auf Basis der Ergebnisse beider tiefenpsychologischen Vorgängerstudien – an KMU-Bedürfnisse angepasst.

Wenn hier im Kontext Awareness von Kampagnen oder Programmen die Rede ist, ist dasselbe gemeint, nämlich in Abgrenzung unverbundener Einzelmaßnahmen eine Verdichtung von Aktivitäten im Sinne integrierter Kommunikation auf Grundlage eines strategisch intendierten Konzeptes, d. h. planvoll bzw. methodisch. Da Security Awareness-Maßnahmen unter anderem als eine Art verlängerter Arm der Security-Protagonisten/-innen zu betrachten sind, bilden diese in größeren Organisationen eine Art Stellvertretendenfunktion aus, d. h. die Botschaften von Maßnahmen übernehmen Teile der Rollen von IT- bzw. Security Manager/-in mit ihren jeweiligen Ansprachen. Je größer eine Organisation, um stärker die Delegation von Kommunikation an Formate und Kanäle der Security Awareness – je kleiner, umso stärker können Bindung bzw. Präventionsbotschaften face-to-face in direkten Dialogen ohne Werkzeuge stattfinden. D. h. dass z. B. in Kleinstunternehmen durchaus die Chance zur direkten Ansprache hinsichtlich Cyber Security genutzt werden soll, bedeutet aber im Umkehrschluss nicht, dass auf Maßnahmen wie die Nutzung der hier vorgestellten Serious Games oder auf ein sauberes Aufsetzen eines Plans im Sinne eines Konzeptes verzichten werden soll. Je größer eine Organisation, umso wichtiger, dass die in diesem Kapitel vorgeschlagenen Module für ein Security Awareness Konzept individuell aufgeladen und genutzt werden.

Die große Chance in KMU besteht darin, dass eine hohe Identifikation und Verbundenheit mit zum Teil engen Bindungen und Produktionsstolz Loyalität schafft und bei der Führung ein hohes Vertrauen in die Mitarbeiter/-innen. Die Kehrseiten des harmonischen Miteinanders einer familiären Kultur wirken sich jedoch zum Teil kontraproduktiv auf die Informationssicherheit aus.

Das Finden von flexiblen Lösungen sowie der vertraute Umgang miteinander vor dem Hintergrund einer überschaubaren Mitarbeitendenrzahl, die diskursive Wissensvermittlung leichter gestalten lassen als in Konzernen, gehören zu den potenziellen Vorteilen der KMU, führen aber gleichermaßen zu kritischen Entwicklungen. Es ist also wichtig, dass die KMU nicht versuchen, Großunternehmen zu kopieren, sondern ihren eigenen Weg mit ihren eigenen Bedingungen und Mitteln finden, um die „Human Firewall“ in ihren Organisationen zu aktivieren bzw. weiter zu stärken. Risikogetriebene ALARMierung ist die eine Seite der Informationssicherheitsmedaille – die andere ist das Aushalten von Fehlern, Kritik und – als eine Stärke von KMU – die Gemeinschaft mit dem KMU-eigenem Produktionsstolz, die es zu sichern gilt, ohne die Kehrseiten zu groß und zu mächtig werden zu lassen [11].

2.1 Security Awareness, Sicherheitskommunikation und -kultur

2.1.1 Definition und Aufgaben von Security Awareness

In Bezug auf das Verständnis von Security Awareness existieren zahlreiche unterschiedliche Definitionen mit zum Teil sehr unterschiedlichen Nuancierungen. Der im Projekt „ALARM Informationssicherheit“ verwendete Begriff unterliegt der folgenden Definition [12]:

Security Awareness ist der Prozess einer methodischen, dauerhaften und nachhaltigen Bewusstseinsbildung bei allen Beschäftigten zum Thema Informationssicherheit mit dem Ziel, diese in einer dem Unternehmen und den Beschäftigten dienlichen Form zu überführen.

Aufgaben von Security Awareness sind u. a. [12]:

- Vermittlung der Security Regelwerke (Policy) und Erklären der dort aufgeführten Regeln
- Vermittlung der Ziele von Informationssicherheit, Aufzeigen der positiven Effekte bei Erfüllung dieser wie auch den möglichen negativen Folgen durch Nichteinhaltung der Regeln
- Reflexion des eigenen Verhaltens: jede/r Mitarbeiter/-in ist mitverantwortlich für die Unternehmenssicherheit (z. B. als Teil einer Human Firewall), inklusive möglicher Konsequenzen bei Nicht-Beachtung von Security-Regeln
- Vermittlung der persönlichen Vorteile, die aus sicherheitskonformem Handeln entstehen
- Kompetenzerwerb bei allen Beschäftigten hinsichtlich der praktischen Anwendung von Security-Regeln inner- und außerhalb des Arbeitsalltags
- Steigerung von Bekanntheitsgrad und Akzeptanz, d. h. Positionierung von Informationssicherheit und Security-Teams durch die nachhaltige Promotion (Förderung) von Security-Themen, -Aufgaben, -Tools und ihren Protagonisten/-innen
- Unterstützung von Führungskräften in ihrer Rolle als Security-Vorbild und -Multiplikator/-in
- Kundenbindung sowie grundsätzlich positive Aufladung des Unternehmensimages (u. a. gegenüber Partnern/-innen, Dienstleistern/-innen, Medien, Governance

und weiteren relevanten Zielgruppen der öffentlichen Wahrnehmung)

Aus Sicht der Zielgruppe setzt die „eigene Awareness“ im Sinne von Bewusstheit vor allem dann an, wenn wir als Menschen bemerken, dass eine Unterbrechung unserer Achtsamkeit in Bezug auf sicheres Verhalten stattfindet und wir gleichsam in der Lage sind, aktiv hierauf zu reagieren, indem wir unser „System“ so steuern, dass wir in der Lage sind, diese Aufmerksamkeit wiederherzustellen – oder wenn dies nicht gelingt – bewusst aus dieser Verfassung herauszutreten. Damit hat Awareness in der Security einen deutlich stärkeren Bezug zum Begriff Awareness, wie er traditionell in der Gestaltpsychologie verankert ist, als zu den rein lerntheoretischen Vorstellungen der Awareness-„Steinzeit“ der Nullerjahre (etwa 2000-2009).

2.1.2 Sicherheitskultur und -kommunikation

Basierend auf diesen zuvor benannten Aufgaben und Dimensionen ist Security Awareness sowohl Teil von Security Marketing und Security Kommunikation, die wiederum dem Begriff der Sicherheitskultur untergeordnet werden [12]. Daraus lässt sich ableiten, dass unter Sicherheitskultur die Gesamtheit der Überzeugungen und Werte von Individuen und Organisationen verstanden wird, bei denen eine Übereinkunft herrscht, welche Ereignisse Risiken darstellen bzw. mit welchen Mitteln diesen Risiken begegnet werden soll [12].Sicherheitskultur unterliegt einem komplexen Lern- und Erfahrungsprozess, in dem sich gemeinsame Ziele, Interessen, Normen, Werte und Verhaltensmuster herausbilden, und ist daher als ein Teil der Unternehmenskultur zu verstehen, an der sichtbar wird, wie Beschäftigte mit Herausforderungen im Kontext Sicherheit umzugehen pflegen. Damit beschreibt sie auch die Art und Weise, wie Sicherheit am Arbeitsplatz organisiert wird, und gibt somit Einstellungen, Überzeugungen, Wahrnehmungen und Werte der Mitarbeiter/-innen in Bezug auf Sicherheit wieder [12]. Der Begriff „Sicherheitskultur“ beschreibt ein dynamisches Phänomen, dessen Ausprägungen sich mit jedem maßgeblichen Ereignis in der Organisation verändern [12]. Dieser Entwicklung muss bei der Implementierung von Security Awareness-Maßnahmen Rechnung getragen werden.

Security Awareness ist – nach der o. g. Definition – mithin Teil der Sicherheitskultur und prägt darüber hinaus diese maßgeblich durch u. a. folgende Faktoren [12]:

- Wahl und Adaption von Konzepten bzw. Frameworks mit Festschreibungen von Intention, Zielen, Methoden
- Kommunizierte Security-Themen
- Kanal- bzw. Medienportfolio
- Zielgruppen bzw. Verfassungen
- Zeitpunkt und Umfang der Maßnahmen
- Art der Ansprache
- Art, Umfang u. Ausgestaltung beim Auftritt, d. h. Security Branding (Sicherheit als Marke)
- Art der Visualisierung
- Tiefe der (inter)kulturellen Diversifikation
- Zusammensetzung, Kompetenz, Zusammenarbeit und Auftritt der Awareness-Organisation und seiner Team-Mitglieder/-innen

2.2 Security Awareness-Treiber

Die im Vorwort beschriebene, zunehmende Cyberkriminalität ist Treiber für zahlreiche Konzepte, Frameworks, Guidelines, Vorgaben u. a. zur Orientierung im Umgang mit Informationssicherheit in Organisationen. Außerdem regeln international anerkannte Standards wie z. B. die ISO/IEC-2700x Anforderungen bzw. Rahmenbedingungen für Informationssicherheits-Managementsysteme (ISMS) mit dem Ziel, Cyberrisiken leichter zu identifizieren, zu analysieren und zu managen, um z. B. Risiken zu minimieren – u. a. auch durch Security Awareness.

Inzwischen gehört Security Awareness zu den gesetzten Bestandteilen der Geschäftsabläufe auf allen Ebenen seriös agierender Organisationen. Gerade Bezugsgruppen wie Gesetzgeber/-innen, Gerichte, Kunden/-innen, weitere Business-Partner/-innen u. v. m. fordern nicht nur generelle Nachweise in Bezug auf Informationssicherheit, sondern zunehmend auch die einer erfolgreichen Sensibilisierung der Mitarbeiter/-innen. Im juristischen Kontext ist dies u. a. für den Fall etwaiger Compliance-Verstöße notwendig [12].

Insbesondere durch das Einhalten von internationalen Standards soll

- Informationssicherheit kontinuierlich verbessert werden,
- Informationssicherheit im Unternehmensalltag verankert werden,
- Informationssicherheit externen Anforderungen gerecht gemacht werden,
- Vertrauen mit Geschäftspartnern/-innen und in der Öffentlichkeit geschaffen werden.

2.2.1 Normfamilie ISO/IEC 2700x

Auch die ISO /IEC 2700x fordert die Schulung der Mitarbeiter/-innen im Bereich der Informationssicherheit und der Security Awareness und definiert die Details einer derartigen Schulung unter dem Standard A.7.2.2 („Information Security Awareness, Education and Training“).

Dort sind insbesondere in den Kapiteln 7.1 bis 7.4 verschiedene Aspekte von Security Awareness beschrieben [13], u. a.

- sichere Arbeitsprozesse
- Affekte, die die Informationssicherheit betreffen
- Aus- und Weiterbildung von Mitarbeiter/-innen

- Erfahrung und Kompetenzen von Mitarbeiter/-innen
- Dokumentation und Wirksamkeitsüberprüfung
- Kommunikations-Themen, -Zeitpunkt, -Zielgruppen, -Absender/-innen und -Methoden

So ist etwa unter Kapitel 7.1 („Ressourcen") u. a. festgelegt [13], dass die Organisation die für die Errichtung und Umsetzung von Informationssicherheit benötigten

- Ressourcen,
- deren Wartung und
- die kontinuierliche Verbesserung des Informationssicherheitsmanagementsystems

bestimmen muss.

Abschnitt 7.2.2 führt unter „Sensibilisierung, Aus- und Weiterbildung für Informationssicherheit" u. a. an: „Alle Mitarbeiter der Organisation und gegebenenfalls Auftragnehmer sollten eine angemessene Sensibilisierung und Schulung sowie regelmäßige Aktualisierungen der Unternehmensrichtlinien und -verfahren erhalten, die für ihre berufliche Funktion relevant sind [13]."

Darüber hinaus ist unter 7.2 definiert, dass die Organisationen im Kontext Informationssicherheit folgende Aspekte berücksichtigen und definieren müssen [13]:

- die notwendigen Fähigkeiten der Mitarbeiter-/innen, die von ihnen zu erledigenden Arbeitsprozesse und die in diesem Kontext möglichen Affekte, die die Informationssicherheit betreffen,
- Zuständigkeit der Mitarbeiter/-innen auf der Grundlage von angemessener a) Ausbildung, b) Weiterbildung bzw. c) Erfahrung;
- Maßnahmen hinsichtlich der Weiterbildung, um gegebenenfalls eine nicht ausreichende, aber notwendige Kompetenz in Bezug auf die Sicherung der Informationssicherheitsziele zu erwerben,
- Dokumentation bzw. Wirksamkeitsüberprüfung getroffener Maßnahmen im Bereich des Kompetenzerwerbs hinsichtlich der Informationssicherheit.

Als Maßnahmenbeispiele werden dort genannt [13]:

- Ausbildung,
- Betreuung bzw. Umstrukturierung von Personal oder
- Einstellung neuer, kompetenter Personen.

Kapitel 3 fordert in Bezug auf Awareness unter 7.3, dass Mitarbeiter/-innen folgende Schlüsselfaktoren bewusst sein sollen [13]:

- die Inhalte der Information Security Policy,
- die Wirksamkeit des eigenen Verhaltens in Bezug auf Informationssicherheit sowie
- die Auswirkungen von Verhalten, das nicht konform ist mit den Anforderungen des Information Security Management.

Konkretere Aspekte einer professionellen Kommunikationsstrategie im Kontext Awareness sind unter 7.4 definiert. Demnach sollen Organisationen die Notwendigkeit interner und externer Kommunikation in Bezug auf das ISMS bestimmen, und zwar [13]:

- Themen
- Zeitpunkt (Anm.: Dramaturgie)
- Zielgruppen
- Absender
- Methoden der Wirksamkeit

2.2.2 Weitere Normen

Auch abseits der ISO /IEC 2700x kommt es in immer mehr Branchen bzw. Bereichen zu spezifischen Frameworks, die Security Awareness, z. T. unter traditionellen Bezeichnungen wie Training oder Schulung, als obligatorisch definieren.

Krankenhauszukunftsgesetz

Das 2021 verabschiedete Krankenhauszukunftsgesetz (KHZG) sicherte Kliniken infolge der COVID-19-Pandemie finanzielle Unterstützung zur generellen Modernisierung zu, u. a. aber auch die Optimierung digitaler Infrastruktur in Krankenhäusern – etwa zur Verbesserung von IT-Sicherheitsmaßnahmen inklusive Security Awareness als ein Fördertatbestand [14].

KRITIS

Weil insbesondere kritische Infrastrukturen (KRITIS), zu denen u. a. auch Krankenhäuser gehören, verstärkt im Fokus von Cyberangriffen stehen und diesen weitreichende Auswirkungen auf Staat, Gesellschaft, Wirtschaft bzw. öffentliche Sicherheit inhärent sind, erfordern diese besonderen Risiken einen expliziten Schutz mit der Vorgabe spezieller Sicherheitsanforderungen durch den Gesetzgeber und etlichen Nachweispflichten in Bezug auf ergriffene Sicherheitsmaßnahmen. Die zentralen Anforderungen sind im IT-Sicherheitsgesetz (IT-SiG) und der BSI-Kritis-Verordnung (BSI-KritisV) dokumentiert. Die zentrale Norm für Betreiber/-innen kritischer Infrastrukturen ist der §8a BSIG, der Maßnahmen und Prozesse sowie Art und Umfang von Nachweisen oder eine Meldepflicht für Sicherheitsvorfälle definiert. Der terminologische Begriffskern im Kontext von KRITIS bildet eine so genannte „gelebte ganzheitliche Sicherheitsstrategie" mit besonderen Aufgaben der Führungsebene nach einem Top-Down Prinzip, das u. a. Förderung und Forderung umfasst und das Thema „Sicherheitskultur" adressiert. Hierzu gehören z. B. die Weiterbildung des Managements und die Förderung von Schulungen aller Mitarbeiter/-innen [15] – mit dieser auch eher traditionellen Umschreibung sind vermutlich nicht nur lerntheoretische Ansätze im Verständnis der Nullerjahre (etwa 2000-2009), sondern sämtliche Security Awareness-Maßnahmen gemeint.

DIN SPEC 27076

Die im April 2023 publizierte DIN SPEC 27076 [16] richtet sich sogar explizit an KMU. Dort wird ab Seite 17 ausdrücklich empfohlen, dass Dienstleister/-innen, die nach dieser Spezifikation kleine Unternehmen in Sachen IT-Sicherheit beraten wollen, die Geschäftsführung sensibilisieren müssen. Im weiteren Verlauf wird außerdem gefordert, dass bei einem Sicherheitsvorfall im Unternehmen allen Mitarbeiter/-innen bewusst sein muss, wie sie sich zu verhalten haben und im Kontext Incident Management wem was und wann zu melden ist [17]. Darüber hinaus sollen „alle Unternehmensangehörigen, die die Unternehmens-IT nutzen, mit der IT und dem Netzwerk sicher umgehen und verdächtige Vorkommnisse und Nachrichten (z. B. Phishing-Mails) identifizieren können. Hierfür bedarf es Einweisungen, Schulungen und Sensibilisierungsmaßnahmen." [16]. Eine Verpflichtung zum Lernen und Wissen mit der Erwartung von Compliance, ohne jedoch Sinnhaftes und Bindung über Involvement mitzubewegen, war zwar noch nie ein erfolgsversprechender (Change-)Treiber von Verhaltensänderung, aber eine Verpflichtung von KMU-Sicherheitsdienstleistern, diese auch in Bezug auf Awareness zu beraten, scheint zielführend, solange das Verständnis der Beratenden nicht im Lerntheoretischen hängengeblieben ist.

2.2.3 Weitere Treiber

Über Gesetze und Regulierungen hinaus sind

- interne Vorschriften und Verfahren,
- interne oder externe Audits
- Cyberversicherungen
- Kundenanforderungen und
- Öffentlichkeit

Treiber für Security Awareness.

Cyberversicherungen

Cyberpolicen schützen bei Security Incidents, unter anderem im Fall des Diebstahls bzw. Verlustes personenbezogener Daten, der Verletzung von Betriebs- und Geschäftsgeheimnissen Dritter oder Cyberangriffe auf das betriebliche Netzwerk. Dabei fordern die meisten Versicherungen eine aktive Rolle der versicherten Unternehmen beim Schutz von Informationen und Infrastrukturen, zu dem auch Security Awareness-Maßnahmen gehören. Das heißt, infolge des Nachweises eigener Maßnahmen können Unternehmen im Schadenfall den Selbstbehalt reduzieren, häufig auch „Awareness-Klausel" genannt. In diesem Kontext kooperieren zahlreiche Cyberversicherungen bereits mit Anbieter/-innen von Schulungsmaßnahmen – oder beteiligen sich sogar als Investor/-in – und definieren Standards auf Basis von Prüfungen und KPIs ihrer Partner/-innen. So heißt es etwa im Kontext der Awareness-Klausel der HDI-Versicherung: „Der VN kann seinen vereinbarten monetären Selbstbehalt um 25 % reduzieren, wenn er im Schadenfall nachweist, dass aktuell mindestens 70 % der versicherten Personen Inhaber sowohl des Cyberführerscheins als auch des Datenschutzführerscheins des Präventionsdienstleisters Perseus Technologies GmbH sind." Und weiter: Der VN kann seinen vereinbarten monetären Selbstbehalt um 75 % reduzieren, wenn im Schadenfall ein durch Perseus Technologies GmbH durchgeführter Security Baseline Check (SBC) (…) vorgelegt werden kann [18]."

Aus Sicht der Awareness gilt die Delegation an eine Cyberversicherung grundsätzlich als problematisch, da sie potenziell die Motivation der Mitarbeiter/-innen in Bezug auf sicheres Verhalten kannibalisiert. Aus Sicht der Führung ist sie durchaus nachvollziehbar. Als ein Wertmutstropfen darf jedoch die affirmative Kombination einer Police mit eher simplifizierten Maßnahmen reiner Lerntheorie bzw. Plattform-Awareness betrachtet werden, auch wenn diese aus Businesssicht eine schlaue Absatzstrategie darstellt. Problematisch ist eine derartige Verzahnung vor allem dann, wenn neben den einer Cyberversicherung inhärenten Maßnahmen für die Kunden/-innen keine Wahlfreiheit in Bezug auf abweichende, potenziell besser zur jeweiligen Sicherheitskultur der Versicherungsnehmer/-innen passende Maßnahmen besteht.

Behörden

Gerade im Bereich KMU werden behördliche Initiativen bzw. Veröffentlichungen über Themen, denen laufende Veränderungen inhärent sind und die untrennbar mit dem Begriff Governance verknüpft werden, im Kontext von Leitkultur deutlich stärker wahrgenommen als in international agierenden Konzernen – z. B. Digitalisierung, Cyber Security, aber eben auch Security Awareness. Gerade dem Bundesamt für Sicherheit in der Informationstechnik (BSI) werden im Kontext Cyber Security bzw. Awareness-Vorbildfunktion von den KMU attestiert. Demgegenüber hat das BSI jedoch bisher trotz Aufforderung an deutsche Unternehmen, Präventionsmaßnahmen durchzuführen, weder eine eigene, individuelle Security Awareness-Kampagne für Mitarbeiter/-innen angeboten, sich noch durch fachliche Veröffentlichungen im Kontext Security Awareness ausgezeichnet – im Gegenteil: auch in den BSI-Publikationen über Prävention wird bis auf wenige Ausnahmen immer wieder die Lerntheorie mit Begriffen wie Training, Lernen, Wissen bemüht, um das Thema zu adressieren [19]. In vielen Fällen wird die vom BSI mitgesteuerte Initiative „Allianz für Cybersicherheit" [20] als Durchlauferhitzer für Content bzw. kostenfreie Präventionsmaßnahmen im behördlichen Kontext von Security Awareness vorangeschickt, wobei über diese Plattform jede/r Anbieter/-in ohne eine Qualitätskontrolle jegliche Maßnahme anbieten und promoten darf, die er selber als Awareness bezeichnet. So entsteht ein buntes, aber methodisch fragwürdiges Sammelsurium, das eher irritiert als sich durch eine Vorbildfunktion auszeichnet. Auch eine vom BSI initiierte

Bürgerkampagne unter dem Teil „einfach aBSIchern“ hat weniger mit den Veränderungsgedanken seriöser Security Awareness gemein und mehr mit klassischer Cyber-Propaganda, die Präventionsleistungen über die Kommunikation plakativer Complianceregeln adressiert [21]. Wenigstens hat auch das BSI intern von der über die Bundesakademie für öffentliche Verwaltung (BAköV) im Bundesministerium des Innern und für Heimat produzierten Security Awareness-Kampagne „Sicher gewinnt“ [22] profitiert, eine Rahmenkampagne für die deutschen Bundesbehörden, das bereits seit 2010 immerhin gamifizierte Formate innerhalb systemische Kommunikationssettings einsetzt. Mit dem Rollen- und Trainingsspielen umfassenden Trainingskoffer [23] des Cybersicherheitsnetzwerk (CSN)], wird jedoch auch im Kontext des BSI ab 2022 der Aspekt Gamification im BSI-Kontext zunehmend kommuniziert bzw. mit Akzeptanz belegt. Und somit der Awareness-Fokus weiter aus der traditionellen Lerntheorie in systemisch-methodische Kontexte verschoben.

Kunden/-innen bzw. Öffentlichkeit

Die kontinuierliche Implementierung von Security Awareness-Maßnahmen reduziert in überprüfbarer Weise nicht nur das geschäftliche Risiko von Unternehmen; sie erhöht darüber hinaus auch deren Attraktivität. Denn sowohl die Zusicherung von Sensibilisierungsmaßnahmen gegenüber Kunden/-innen und Partnern/-innen als auch deren externe Kommunikation sichern den Unternehmen Wettbewerbsvorteile, weil sie positive Imagefaktoren generieren und das Vertrauen in das Unternehmen erhöhen [12].

In Bezug auf Kunden/-innen und Partner/-innen

- Einladung zu Awareness-Veranstaltungen, um externen Gästen (innovative) Formate, hohe Beteiligung und sichtbare Erfolge zu demonstrieren
- Format-Sharing durch Weitergabe von Good Practice
- Gemeinsame Entwicklung von Formaten als Projekt
- Weitergabe evaluierter Nachweise z. B. durch KPIs, um Anforderungen aus Verträgen zu erfüllen

In Bezug auf Öffentlichkeit, z. B. insbesondere via Medien:

- Reputationssteigerung durch besonders anschauliche Verwertung von Awareness-Maßnahmen als Repräsentant von Informationssicherheit und Datenschutz
- Beleg von Awareness- bzw. Sicherheits-Know-how durch Veröffentlichung, z. B. PR, oder aktive Teilnahme an Awards bzw. Fachkongressen

Leider ist auch in Bezug auf Veröffentlichungen in z. B. Fachmedien festzustellen, dass bei Beiträgen über Security Awareness der Awarenessbegriff noch heute stark von den Vorstellungen über die Lerntheorie der Nullerjahre (etwa 2000-2009) geprägt ist und Awareness – ähnlich wie in den mit Normen verknüpften oder von Behörden bzw. aus Governance-Bereichen initiierten Publikationen in diesen überwiegend auf Training, Lernen, Wissen reduziert wird.

2.2.4 Zwischenfazit: Vorteile von Security Awareness

Als Teil von Sicherheitskommunikation ist Security Awareness eine Voraussetzung für erfolgreiches Security Management. Mit der Umsetzung wirksamer und nachhaltiger Security Awareness-Maßnahmen ergeben sich verschiedene Benefits für Unternehmen [12]:

- Belegbare Verbesserung der Sicherheitskultur durch Übernahme von Verantwortung mit der Stärkung (Empowerment) von Beschäftigten in Bezug auf Informationssicherheit, der Reduktion von Sicherheitsvorfällen (Security Incidents) und der unternehmensweiten Steigerung von Akzeptanz gegenüber jeglicher Form von Sicherheitsmaßnahmen.
- Mögliche Unterstützung bei Audits, z. B. im Rahmen von ISO /IEC 27001-Zertifizierungen durch nachweisbare Awareness-Maßnahmen bzw. Kennzahlen.
- Innovative und effektive Security Awareness-Maßnahmen unterstützen Bezugsgruppenbindung (Mitarbeiter/-innen, Kunden/-innen, Partner/-innen, Medien, Öffentlichkeit etc.) und fördern das Geschäft, da darüber die Bedeutung von Sicherheit im Unternehmen deutlich wird.
- Image, geschäftliche Reputation und Marktwert werden aufgrund belegbarer Awareness-Maßnahmen, Good Practice Sharing, Vorträgen, Sicherheitspreisen etc. verbessert.
- Positive Rückkopplungseffekte nach innen durch externe Veröffentlichungen und Auftritte (z. B. über Konferenzen u. a. Fach-Events)

2.3 Aufgaben und Methoden der Security Awareness

Aufgaben von Security Awareness sind u. a.:

- Vermittlung den Security Policy und Erklären der dort aufgeführten Regeln
- Vermittlung der Ziele der Informationssicherheit und der positiven Auswirkung auf das Unternehmen bei Erreichen der Ziele und – umgekehrt – der negativen Folgen der Nichteinhaltung der Regeln
- Vermittlung der Wirksamkeit des eigenen Verhaltens, d. h. dass jede/r Mitarbeiter/-in als Teil einer Human Firewall verantwortlich für Sicherheit ist, inklusive möglicher Konsequenzen bei Nicht-Beachtung von Security-Regeln
- Vermittlung der persönlichen Vorteile, die durch sicherheitskonformes Handeln erzeugt werden
- Vermittlung von Kompetenzen bei allen Beschäftigten hinsichtlich der praktischen Anwendung von Security-Regeln innerhalb des Arbeitsalltags
- Positionierung von Informationssicherheit und Security-Teams durch die nachhaltige Promotion

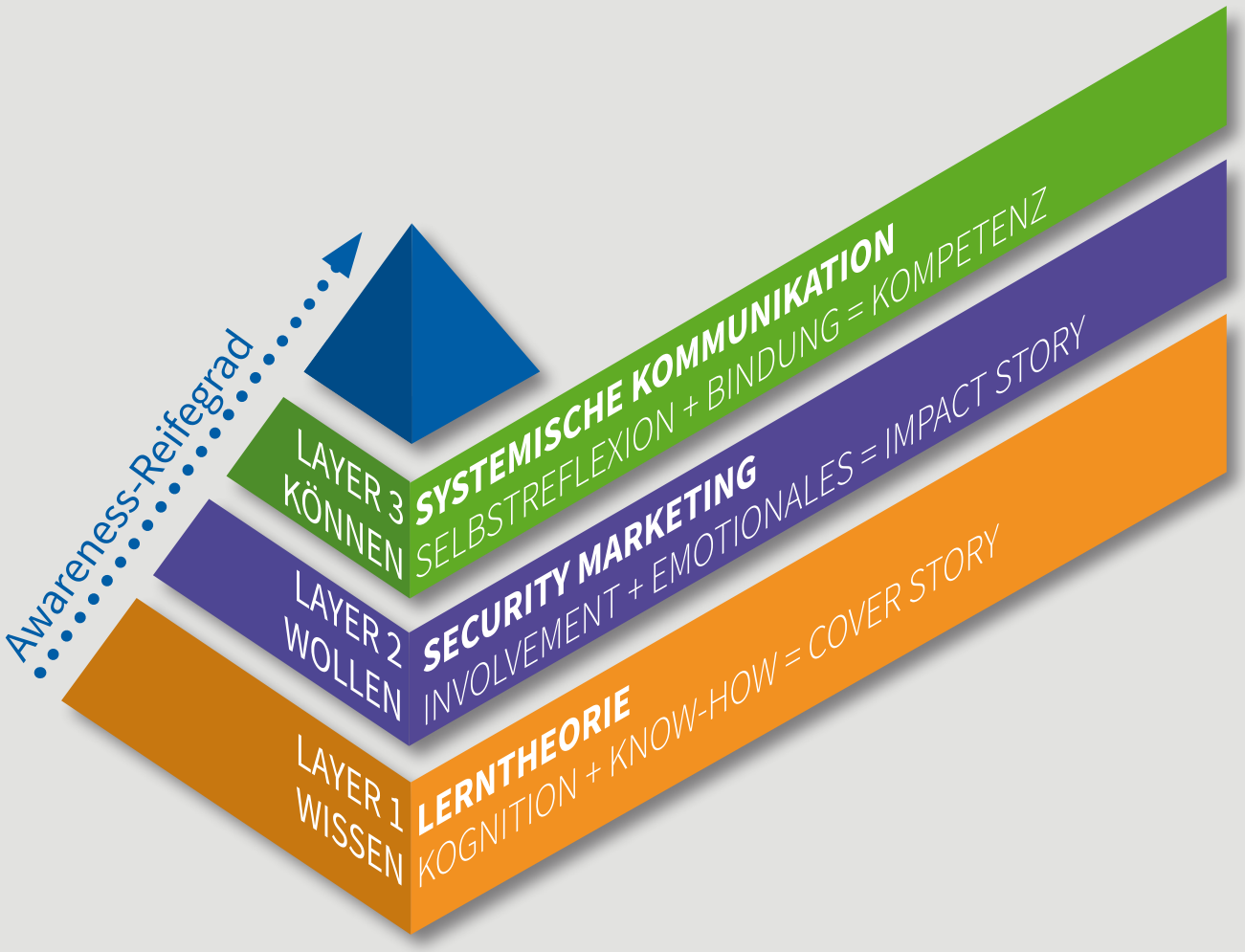


Abb. 6: *Security Awareness Layer-Modell nach Helisch/Pokoyski (Quelle: known_sense)*

von Security-Themen, -Aufgaben, -Tools und -Protagonisten/innen mit dem Ziel Bekanntheit und Akzeptanz zu steigern
- Unterstützung von Führungskräften, damit diese ihren Aufgaben als Security-Vorbild und -Multiplikator/-in gerecht werden können
- Kundenbindung sowie grundsätzlich positive Aufladung des Images der Organisation– dies u. a. gegenüber Partnern/-innen, Dienstleistern/-innen, Medien, Governance und weiteren relevanten Zielgruppen der öffentlichen Wahrnehmung

Basierend auf diesen Aufgaben, ist Security Awareness als ein multidisziplinärer Bereich Teil der Sicherheitskultur von Organisationen [12].

Das heißt, die Schlüsselfaktoren von Security Awareness weisen Überschneidungen auf zum betrieblichen Bildungsmanagement bzw. zur Personalentwicklung, zur generellen Security-Kommunikation sowie zum Veränderungsmanagement und prägen die drei methodischen Ebenen von Security Awareness[12]. known_sense spricht in diesem Kontext von so genannten „Layern) [24]:

- **Wissen** (Elemente aus der Lerntheorie, kognitive Faktoren)
- **Wollen** (Elemente aus dem Marketing, emotionale Faktoren)
- **Können** (Elemente von Veränderungsmanagement bzw. systemischer Kommunikation)

2.3.1 Ebene 1: Wissen (Lerntheorie)

Die klassische Kognition (Informationsverarbeitung) bildet die (Old School-)Grundlage von Security Awareness [12], mit der (lediglich) eine informelle Wissensvermittlung in Bezug auf Security-Regeln, Richtlinien (Policy), Sicherheitsrisiken und mögliche Folgen von Sicherheitsverstößen auf einer sichtbaren, d. h. nachweisbaren, faktischen Ebene (Cover-Story) [25] stattfindet.

2.3.2 Ebene 2: Wollen (Marketing)

Da Sicherheits- und Fehlerkultur ihren Ursprung in der Regel auf einer unbewussten, häufig nicht sichtbaren Ebene (Impact-Story) [25] haben und die reine Informationsvermittlung nicht ausreicht, um in Awareness-Prozessen eine nachhaltige, gerade auch motivierende Wirkung auszuüben, müssen bei sämtlichen Zielgruppen auch emotionale Faktoren über das Marketing adressiert werden (Ebene 2) [12].

2.3.3 Ebene 3: Können (systemische Kommunikation)

Sicherheit umfasst im Sinne einer Interaktion aller Protagonisten auch systemische Faktoren, deren Besonderheiten in der Ebene 3 (Können) sich produktiv über systemische Kommunikation fördern lassen („Empowerment“, d. h. die Verstärkung von Autonomie bzw. Selbstbestimmung) [12]. Denn das Verhalten von Individuen wird stets geprägt von dem sozialen Gefüge, in dem es sich bewegt. Je mehr Bewusstsein dafür besteht, dass die Art der Beziehungen und das soziale Miteinander das Verhalten aller beeinflussen, z. B. die Fehlerkultur, desto größer ist die Chance, dass Menschen sich sicherheitskonform verhalten, auch wenn es ihnen emotional gegebenenfalls schwerfällt. Um diese soziale Ebene zu modellieren, eignen sich insbesondere dialogische Konstellationen (z. B. Teamformate) mit dem Ziel, soziale Handlungskompetenzen und einen für Awareness notwendigen Sicherheitsdiskurs unter den Beteiligten zu fördern. Erst die durch das Marketing bedingte emotionale Ansprache (Ebene 2) und das systemische Einüben von Security relevantem Verhalten (Ebene 3) ermöglicht das Abrufen der Wissensbasis aus Ebene 1 [26].

2.3.4 Formate und Instrumente der drei Layer

Formate und Instrumente der Ebene 1 sind z. B.

- klassisches E-Learning (z. B. Web Based Trainings)
- klassische Präsenztrainings (Classroom-Ansatz)
- klassischer Textcontent (z. B. News oder Artikel in Corporate Media wie etwa Intranet oder Mitarbeitermagazin, FAQs, Wikis)
- Quickinfos (z. B. via E-Mail) bzw. Newsletter

Formate und Instrumente der Ebene 2 sind z. B.

- Flyer und Quick Guides (z. B. mit verkürzten Regelwerken, Goldene Regeln, Tipps & Tricks)
- Poster, Aufsteller, Displays u. a. Visuals (z. B. Intranet-Banner)
- Sticker, Badges & Co.
- Videos, Animationen (z. B. Erklärfilme)
- Audio-Podcasts oder -Hörbücher
- Mitarbeiter-Events, Roadshows
- (Gamifizierte) Mitarbeiter/-innen-Wettbewerber/-innen
- Giveaways und Incentives
- Digitale Minigames, Online Team Games
- Security Brand-Elemente (Key Visual, Leitfiguren, Claim, konsistentes Wording und Naming)
- Comics, Cartoons, weitere Bildergeschichten & Co.
- Externe Promotion von Awareness-Maßnahmen, z. B. über Good-Practice-Sharing, Fachkongresse oder PR (inklusive Rückkoppelungseffekte nach innen)
- weitere (klassische Marketing-)Tools

Formate und Instrumente der Ebene 3 sind z. B.

- Moderationsinstrumente für diskursive Team-Settings, z. B. Moderationskartensets, Lernkarten bzw. Infografiken

SECURIBILITY – AUF WELCHEN LAYERN WIRKT SICHERHEITS-KOMMUNIKATION?

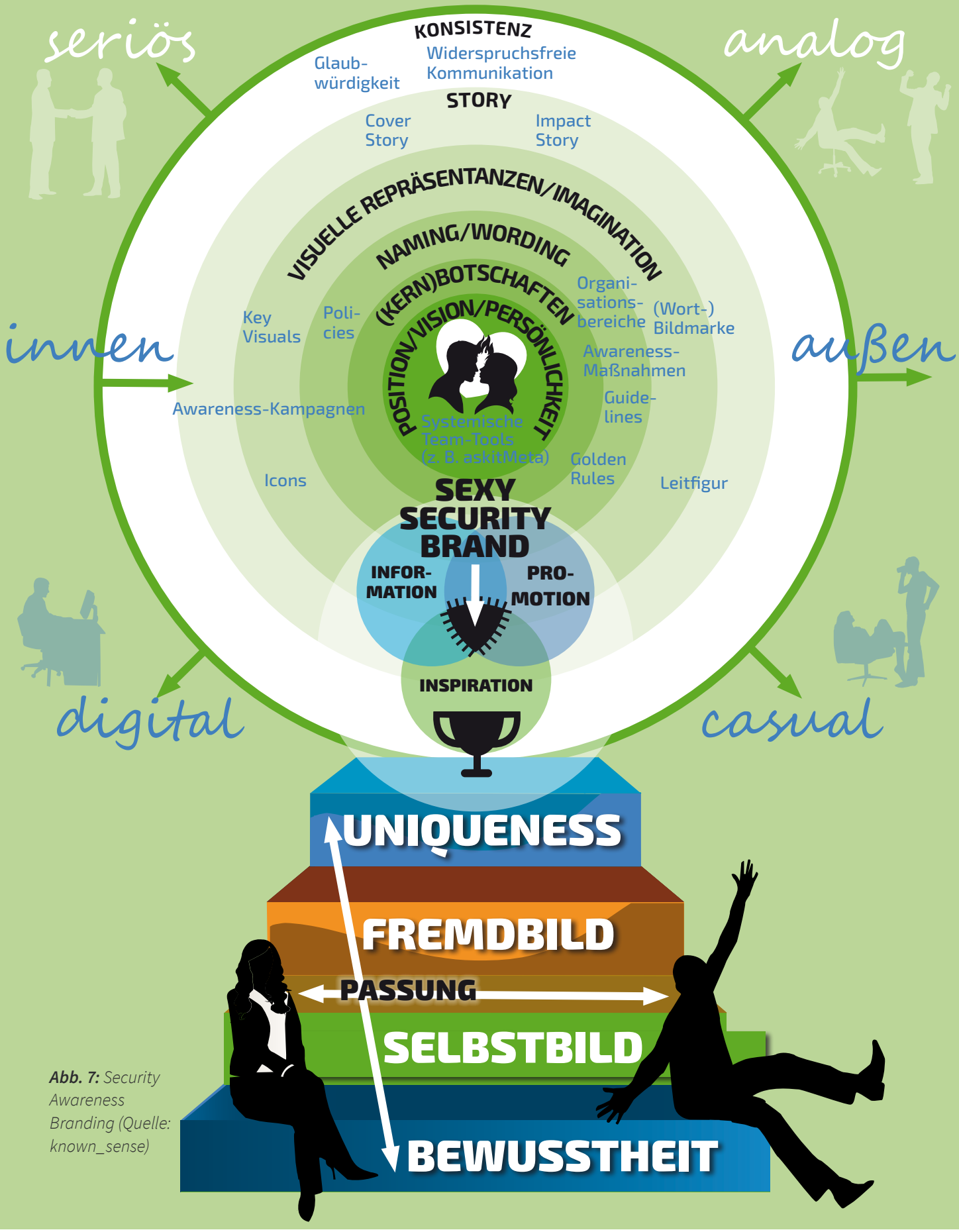


Abb. 7: *Security Awareness Branding (Quelle: known_sense)*

- Deep Dive Workshops u. a. zielgruppen-spezifische Intensivtrainings mit gamifizierten Simulationen und weiteren diskursiven bzw. interaktiven Elementen
- Analoge Serious Games, z. B. Simulationen, Lernstationen, Edutainment- und Planspiele
- Digitale Serious Games (mit diskursiver Nachbereitung)
- (interaktive) Aktionen, (Selbst-)Tests, Assessments
- Talk Shows, Town Hall Meetings
- Guerilla Marketing (über das man spricht)
- Security Awareness-App (mit Rückkanal)

Eine derartige Typologie von Formaten existiert nicht in Reinform [12]. D. h. die im Projekt „ALARM Informationssicherheit“ zu entwickelnden Lernszenarien sind grundsätzlich der Ebene 3 zuzuordnen und umfassen gleichzeitig didaktische und emotionale Awareness-Leistungen aus den Teildisziplinen Lerntheorie (Ebene 1) bzw. Marketing (Ebene 2). Aus zahlreichen internen, tiefenpsychologischen Studien bei known_sense-Kunden/-innen (z. B. „Tiefenpsychologische Konzeptanalyse mySecurity & Privacy Box bei T-Systems International“) [27] sowie quantitativen Erhebungen im Kontext qualitativer und quantitativer Erfolgsmessung, die known_sense für weitere Kunden/-innen intern produziert hat, ergaben sich wichtige Faktoren für die Umsetzung der Methoden. Sämtliche Ebenen sollten wechselseitig im Sinne einer widerspruchsfreien Kommunikation an einer Kampagne beteiligt sein. D. h. auch, dass jedes Instrument mit jedem anderen verbunden sein sollte; die einzelnen Formate sollten auf die jeweils anderen einzahlen (d. h. für diese werben). Darüber hinaus muss ein diverses Portfolio an Formaten bereitgestellt werden, das unterschiedliche Lerntypen bzw. Zielgruppen und psychologische Verfassungen anspricht. Nachhaltige Security Awareness entsteht am Ende dann, wenn sämtliche Layer wechselseitig an einer Kampagne beteiligt sind.

2.4 Security Awareness Branding

Um über die einzelnen Module nachhaltig positive Kollateraleffekte zu erzielen, eine einwandfrei identifizierbare Verbindung herzustellen und die Identifikation mit den Maßnahmen bzw. die Aufmerksamkeit der Zielgruppen grundsätzlich zu heben, empfiehlt sich für die Kommunikation ein eindeutiges, internes Branding. Dieses sollte ein konsistentes Wording und Naming und auch narrative Ansätze eines Storytelling zur Erstellung von z. B. Leitfiguren bzw. Leitfiguren-Familien enthalten, aus denen dann etwa Avatare für die Moderation innerhalb von Lehr- oder Erklärmedien oder Geschichten über Sicherheit in Comics o.ä. hergeleitet werden können.

Ein Branding-Teil sollte ein Kapitel eines seriösen, auf Nachhaltigkeit bedachten Awareness-Konzeptes ausmachen und u. a. folgende Details umfassen.

- Naming bzw. Wording
- Kampagne
- Leitfigur (optional)
- Slogan bzw. Claim
- Kernbotschaft(en)
- generelle Security-Semantik, insbes. Auftritt der Sicherheits-Organisation, Formulierungen der Policies und Guidelines, Benennung der einzelnen Kampagnen-Maßnahmen, Zuspitzung von u. a. Policy-Promotion durch Reduktion der Textmenge von Regeln bzw. Erklärung dieser, z. B. mithilfe leicht verständlicher Kernbotschaften
- Visualisierung
- Leitfigur (bzw. – daraus hergeleitet – ggf. Figurenfamilie)
- Key Visual (eine Art Kampagnen-Logo bzw. -Icon als Bildmarke, Wortmarke oder Wort-Bildmarke)
- weitere Security Visuals
- Storytelling auf zwei Ebenen:
  - An der Oberfläche: die offiziell-plakative, im Vordergrund stehende Cover Story als eine (be) greifbare, nacherzählte und unmittelbar plakative Geschichte mit konkreten Informationen über die Kampagne und deren Inhalte
  - Im Hintergrund: die „versteckte“, nicht sofort erzählbare, aber stets spürbare Impact Story als ein psychologisches Fundament mit tragender Verfassung

Story, Ansprache, Leitfigur und Key Visual

Das Key Visual soll ggf. aus einer sprechenden, gut wiedererkennbaren und sympathischen Leitfigur hergeleitet werden, die alle Kampagnenmaßnahmen und auch die Sicherheitsprotagonisten/-innen als verantwortliche/n Absender/-in repräsentiert und als Teil eines authentischen, zur Informationssicherheit passenden Narrativs konstruiert wird, auch um erklärungsbedürftige Security-Inhalte bzw. -regeln mithilfe einer simplifizierten Umgebung, z. B. Comic o.ä., darzustellen. Sie soll demnach hinsichtlich konkreter narrativer Instrumente als Absender/-in (im Sinne eines Avatars oder Maskottchen etc.) genutzt werden. Dabei ist ggf. nicht nur eine einzige Figur, sondern eine komplette Figurenfamilie notwendig, mit der die Leitfigur auf der „Awareness-Bühne“ interagiert [28].

Als Leitfigur kommen theoretisch infrage:

- Mensch (z. B. in einer bestimmten Rolle, etwa Superheld oder Sicherheitsbedürftige/r)
- Tier (vermenschlicht)
- Objekt (vermenschlicht)
- Mischwesen

Ein Comic braucht i. d. R. zum/zur Hauptakteur/-in eine/n Gegenspieler/-in („gut“ vs. „böse“) bzw. eine gegenüber der Organisation simplifizierte, alltagstaugliche Umgebung, in der authentisch zum Thema Informationssicherheit agiert

wird, z. B.

- Haus (oder Teile daraus, z. B. Keller)
- Schiff/Insel
- Himmel (Wolken/Cloud o.ä.)
- Filmstudio
- etc.

Unterstützung erhalten IT- und Security-Bereiche in der Regel von der internen Kommunikation. Leitfiguren müssen auch nicht zwingend von Agenturen entwickelt werden, sondern könnten kostengünstig aus Stocks bezogen werden.

2.5 Zielgruppen

Bei der Implementierung von Awareness-Maßnahmen sind die unterschiedlichen Zielgruppen zu berücksichtigen. Einfluss auf eine Segmentierung haben u. a. Faktoren wie

- Beruf
- Aufgabe bzw. Bereich
- Hierarchiezugehörigkeit
- Allgemeinbildung und IT-Verständnis
- Medienverwendung und -verfassungen
- Alter und Länge der Zugehörigkeit zur Organisation
- Geschlecht
- soziale bzw. kulturelle Herkunft
- Einstellungen
- Nationalität

Besonders als Zielgruppen für individuelle Maßnahmen hervorzuheben sind

- HR-Mitarbeiter/-innen (Bewerbungen zahlreicher unternehmensfremder Personen)
- Controler/-innen bzw. Buchhalter/-innen, Geschäftsassistenzen, Sekretariat, Empfangspersonal (umfangreiche Kontakte zu Externen)
- Auszubildende (besonderes Verhältnis zur Digitalisierung aufgrund des Alters)
- IT-Mitarbeiter/-innen (Admin-Rechte, prägende Beziehung zum Thema Sicherheit)
- Manager/-innen u. a. Führungskräfte (Vorbildfunktion)

Führungskräfte mit Personalverantwortung benötigen, gerade aufgrund ihrer Funktion als Sicherheits-Vorbild besondere Instrumente, die

- ihnen einen Kompetenzvorsprung garantieren
- sie in ihrer Managementfunktion sowie als Vorbild auszeichnen
- ihnen ermöglichen, Awareness-Instrumente zu bewerben sowie
- ihre Teams in das Thema Sicherheit zu involvieren und dafür zu sensibilisieren.

Zu den Instrumenten, die speziell für Führungskräfte entwickelt werden, gehören

- Management-Workshop-Formate,
- Dokumente, in denen die Erwartung an und Pflichten gegenüber Managern/-innen in Bezug auf Informationssicherheit und Awareness geregelt sind,
- Awareness-Ambassador-Konzepte
- Moderationsinstrumente für Team-Sessions.

Bei der Entwicklung bzw. Einführung derartiger Formate ist darauf zu achten, dass diese ihre Zielgruppe auf einer (vordergründigen) Cover-Ebene abholen und offen bzw. unmittelbar Benefits im Umfeld der eigentlichen Managementaufgaben verheißen. Awareness darf dann durchaus verdeckt auf einer Impact-Ebene kommuniziert werden [12].

Bei umfangreicheren Awareness-Kampagnen geraten deutlich mehr unterschiedliche Zielgruppen in den Fokus der Betrachtung, KMU sollten sich jedoch auf die oben genannten, wichtigsten Zielgruppen beschränken. Darüber hinaus ist zu beachten, dass die so genannte Zielgruppe an sich als rein sozialwissenschaftliches Modell in der Werbewirkungsforschung immer häufiger von Persona und psychologischen Verfassungen abgelöst wird, von denen wir als Akteur/-in im Tagesverlauf mehrere durchlaufen. Die detaillierte Betrachtung von Verfassungen würde jedoch den Rahmen dieses Dokuments und die Möglichkeiten von KMU sprengen, während Persona nichts anders darstellen als Zielgruppen mit konkreten Zuschreibungen von Biografien und Eigenschaften.

2.6 Awareness-Organisation und -Rollen

Eine Security Awareness-Kampagne sollte durch ein zentrales Awareness-Team entwickelt und betreut werden, das Awareness-Services für alle Bereiche der Organisation liefert. Seine primäre Funktion ist die ständige Pflege, Verbesserung und Kontrolle der Methoden und Konzepte. Dazu gehört auch die Auswahl, Anpassung, Erstellung und Implementierung von Awareness-Instrumenten inklusive Beratungsleistungen bei allen internen Fragen.

Falls im jeweiligen KMU ein Security-Bereich existiert, ist dieser die logische Adresse zur Bildung und Steuerung eines Awareness-Teams, andernfalls könnten IT- oder Kommunikationsbereiche oder aber die Geschäftsleitung selbst diese Funktion übernehmen. Bei einer Diversifikation auf mehrere Standorte sollten lokale Zuständigkeiten mitbedacht werden.

Zur Durchführung von Security Awareness-Maßnahmen müssen Teams bzw. Personen über ein Minimum an Fähigkeiten und Erfahrung in Bezug auf Awareness und im Sinne der drei Layer von Security Awareness insbesondere über folgende methodische Ansätze verfügen:

- Lerntheorie (Layer 1: Wissen)
- Marketing (Layer 2: Wollen)

- Systemische Kommunikation (Layer 3: Können)

Sie müssen hinsichtlich der klassischen Kommunikation ebenso ein Minimum an Fähigkeiten und Erfahrung einbringen in Bezug auf folgende kommunikative Detailschritte:

- Konzept,
- Steuerung von Medienproduktionen bzw. Beschaffung, z. B. im Kontext von Agentur-Dienstleistungen wie Kreation, Inhalts-Erstellung, Design,
- Roll-out,
- Projektmanagement,
- Wirksamkeitsnachweise und Dokumentation

sowie Kenntnisse über die Teilaspekte

- Security Painpoints (Themen und Inhalte)
- Zielgruppen
- verfügbare Kanäle, Formate und Medien

Darüber hinaus werden Security Awareness-Maßnahmen verbessert über die Integration zusätzlichen Experten-Know-hows in den Disziplinen:

- Psychologie bzw. Wirkungsforschung
- Supervision und Coaching
- Inhalts-Erstellung (Text, Bild) bzw. Redaktion
- Produktentwicklung
- Storytelling
- Markt- und Medienforschung
- etc.

Eine unzureichende Qualifikation der für Awareness verantwortlichen Personen kann den Erfolg von Awareness-Maßnahmen gefährden. Für KMU empfiehlt es sich, Teams mit internen Experten/-innen zusammenzustellen, um möglichst viele der oben beschriebenen Skills abzudekken. Psychologisches Know-how kann vermutlich am besten über ein externes Coaching bzw. Challenging der Gesamtaktivitäten eingekauft werden.

2.7 Awareness-Lebenszyklus und Konzept Management

2.7.1 Awareness-Lifecycle

Der Lebenszyklus beim Awareness-Prozess läuft in der Regel nach folgendem Schema ab:

1. Bedarfsermittlung und Definition von Zielerreichung, aktuellen Risiken, Incidents, Sicherheitskultur
2. Positionierung auf Basis des hiesigen Leitfadens und unter Berücksichtigung von Beratung durch das zentrale Awareness-Team – z. B. bezüglich Methoden, Formate etc.
3. Konzepterstellung im Mix verfügbarer Instrumente und Individualentwicklungen (z. B. Detailkonzepte für Verantwortlichkeiten, Entwicklung, Implementierung, Projektmanagement berücksichtigen)
4. Promotion bei der Geschäftsleitung hinsichtlich Unterstützung und Budget
5. Bereitstellung von Ressourcen und Budget
6. Nutzung verfügbarer Instrumente wie die Formate aus „ALARM Informationssicherheit“ und Entwicklung bzw. Einkauf von neuen, individuellen Instrumenten
7. Rollout bzw. Implementierung der gewählten Instrumente
8. Auswahl, Konzept, Entwicklung, Rollout von Promotions-Instrumenten (Sekundärinstrumente) für die Werbung der ausgerollten Primärmaßnahmen
9. Dokumentation und Reporting
10. Evaluation mit anschließender Optimierung und neuer Bedarfsermittlung bzw. Zielerreichung

2.7.2 Awareness-Konzept und -Dokumentation

Ein laufendes Awareness-Konzept unterstützt die vollständige Implementierung von Awareness-Aktivitäten innerhalb der jeweiligen Organisation Das langfristige Ziel des Awareness-Konzeptes ist die Erfüllung der geschäftlichen Anforderungen an die Organisation durch u. a. die nachhaltige Verbesserung der Awareness bei sämtlichen Beschäftigten, nachweislich auf Basis einer Evaluation bzw. von regelmäßigen Reviews der Einzelmaßnahmen, die nach erfolgreicher Implementierung zu dokumentieren sind.

Das Awareness-Konzept ist ein dynamisches und lernendes Konzept, das permanent fortgeschrieben wird auf Basis u. a. folgender Faktoren:

- eine sich ändernde Sicherheitskultur
- eine sich ändernde Risikolandschaft mit immer neuen bzw. angepassten Angriffsvektoren
- sich ändernde Geschäfts- bzw. Kundenanforderungen
- Veränderungen in der Beschäftigtenstruktur
- Innovationen in Bezug auf Methoden und Tools
- Ergebnisse der Evaluation
- Erfahrungen, Erfolge oder Misserfolge bei Einzelmaßnahmen

2.8 Security Awareness-Reifegrad und Wirksamkeits-Überprüfung

Für die Wirksamkeits-Überprüfung stehen unterschiedliche quantitative und qualitative Methoden diverser Anbieter/-innen zur Verfügung. Es spricht jedoch nichts gegen die Inhouse-Erstellung von Fragebögen. Auf der Webseite des Projektes „ALARM Informationssicherheit“ werden entsprechende Hilfsmittel als Download zur Verfügung gestellt.

Eine Übersicht über Reifegrad-Modelle und Tools bietet die

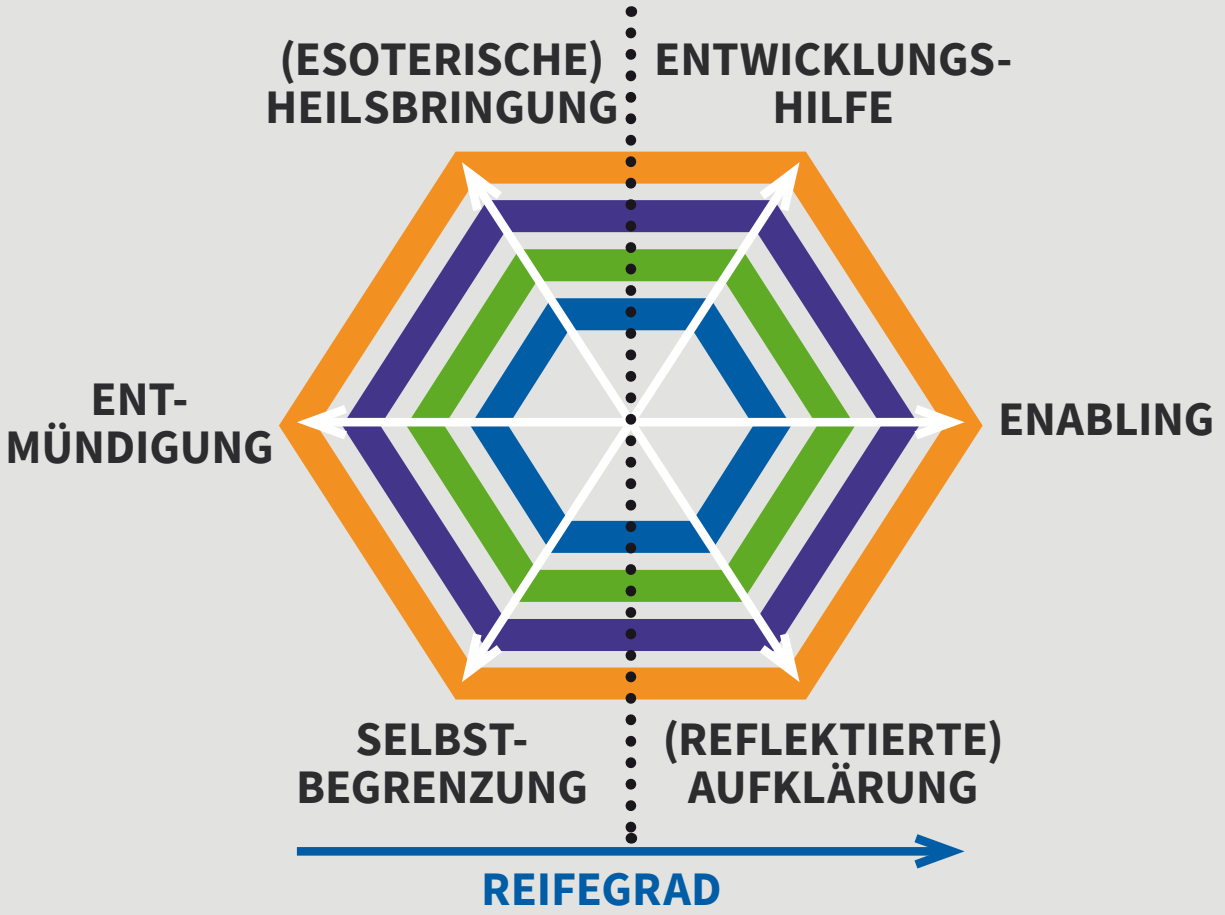


Abb. 8 und 9: *Psychologische Grundspannung Security Awareness und Nutzung von LS bzw. anderen diskursiven Tools in KMU (Grafik 3 von 3, oben, Quelle Studie 2 aus 2022 [29]) und Lebenszyklus Security Awareness (unten, Quellen: known_sense)*

ALARM-Studie „Enabling vs. Entmündigung. Qualitativer Konzepttest analoger Security Awareness-Lernszenarien für KMU im Projekt „ALARM Informationssicherheit“ [29]“ ab Seite 51.

Ausgehend von den bisher bekannten Konzepten und dem Layer-Modell von known_sense, dargestellt u. a. in der KMU-Grundlagenstudie [11] auf S. 15, und basierend auf der damit verbundenen Evaluation, kann für KMU im Folgenden ein vereinfachtes Positionierungs-Modell eines Reifegrads skizziert werden, das eben Awareness nicht nur auf Training begrenzt, sondern über die Lerntheorie hinaus auch Marketing-Faktoren, psychologische Dimensionen und solche der systemischen Kommunikation zu integrieren versucht.

Awareness-Reifegrad = 0: Die Organisation ist so restriktiv und in Bezug auf Digitalisierung wenig agil aufgestellt, dass die Bezugspunkte für Awareness-Maßnahmen komplett fehlen (oder Awareness ist aus anderen Gründen vollständig mit Reaktanz belegt).

- **Awareness-Reifegrad = 1:** In der Organisation wurden bisher keine Awareness-Maßnahmen durchgeführt, es ist jedoch geplant, Maßnahmen einzuführen.
- **Awareness-Reifegrad = 2:** In der Organisation existieren Awareness-Maßnahmen auf „niedrigem“ Niveau einer z. B. reiner Wissensvermittlung (z. B. Layer 1: Lerntheorie).
- **Awareness-Reifegrad = 3:** In der Organisation existieren Change- bzw. Awareness-Maßnahmen auf „mittlerem“ Niveau, die z. B. neben einem reinen Wissensvermittlung auch werbliche Aspekte berücksichtigt (z. B. Layer 2: Marketing).
- **Awareness-Reifegrad = 4:** In der Organisation existieren bereits Change- bzw. Awareness-Maßnahmen auf einem „höheren“ Niveau, die z. B. neben reiner Wissensvermittlung und werblichen Aspekten diskursive Settings und/oder Gamification als Kommunikationsbeschleuniger berücksichtigt (z. B. Layer 3: systemische Kommunikation). [29].

Aus dem Ranking ergeben sich unter anderem folgende Aufgaben hinsichtlich einer produktiven Implementierung von Security Awareness und insbesondere analogen Serious Games:

- **Awareness-Reifegrad = 0:** Keine, denn der Organisation fehlt der kulturelle Grip für Security Awareness vollständig. Wer abdichtet, legt jede Form einer durch Awareness intendierten Weiterentwicklung lahm, Serious Games inklusive.
- **Awareness-Reifegrad = 1:** Die Organisation verfügt über keine Sensibilisierungserfahrung – bei einer beabsichtigten Nutzung ist auf Serious Games mit geringerer Komplexität zu achten bei gleichzeitiger Einführung von lerntheoretischen Maßnahmen und – in einem weiteren Schritt – von Awareness-Marketingmitteln.
- **Awareness-Reifegrad = 2:** Die Organisation verfügt über Sensibilisierungserfahrung per Lerntheorie – bei einer beabsichtigten Nutzung ist auf Serious Games mit geringerer Komplexität zu achten bei gleichzeitiger Einführung von Awareness-Marketingmitteln.
- **Awareness-Reifegrad = 3:** Die Organisation verfügt über Sensibilisierungserfahrung per Lerntheorie und Marketing – bei einer beabsichtigten Nutzung ist auf Serious Games mit geringerer und mittlerer Komplexität zu achten.
- **Awareness-Reifegrad = 4:** Die Organisation verfügt über Sensibilisierungserfahrung per Lerntheorie, Marketing und systemischer Kommunikation – einer beabsichtigten Nutzung von Serious Games, auch mit hoher Komplexität, steht nichts im Weg [29]

2.9 Entscheidende Schlüsselfaktoren

Folgende Erfolgsfaktoren können hinsichtlich der nachhaltigen Wirkung von Security Awareness Maßnahmen zusammenfassend identifiziert werden [12]:

- Sicherheitskultur beachten und Sicherheit als Marke betrachten
- Geschäftsführung als Unterstützer/-in gewinnen (falls die Awareness-Aktivitäten nicht von dieser ausgehen)
- Führungskräfte als Vorbilder und Multiplikatoren/-innen einsetzen und von Ihnen Zeit-Ressourcen für die Beschäftigten aus ihren Teams gewinnen
- Weitere Unterstützer/-innen gewinnen (z. B. aus Kommunikation, HR etc.)
- Zielführende Methoden mit hohem Synergiefaktor einsetzen – dabei die Awareness-Layer 1-3 berücksichtigen
- Customizing – für verschiedene Zielgruppen zahlreiche verschiedene Kanäle einsetzen
- Maßnahmen bewerben, dokumentieren und soziale Lobbyarbeit betreiben – Security Awareness braucht Werbung und im Sinne von „Sozialarbeit“ eine/n Kümmerer/-in, der/die das Thema „auf die Unternehmens-Straße“ bringt und treibt
- Maßnahmen evaluieren und daraus Bedarfe ableiten
- Persönliche Benefits für alle Zielgruppen vermitteln und dabei eine klare und authentische Ansprache wählen

Abb. 10 und 11: *Analoge Serious Games 3.3.1 (oben) und 3.3.2 (unten)*

3. Die Serious Games des Projektes „ALARM Informationssicherheit“

In diesem Kapitel wird zunächst die grundlegende Methodik bei der Nutzung analoger Serious Games anhand von Lernstationen vorgestellt – inklusive der Grundzüge einer Moderation – und danach die analogen bzw. digitalen Serious Game innerhalb des Projektes „ALARM Informationssicherheit“ mit dem Zusammenwirken beider bzw. mit weiteren Awareness-Formaten.

3.1 Die Lernszenarien-Methodik der analogen Serious Games

Bei einem typischen Lernstation-Training durchlaufen Teams synchron verschiedene Themenstationen, an denen sie von Moderierenden hinsichtlich verschiedener Sicherheits-Themen sensibilisiert werden. Bei der synchronen Verzahnung von Lernstationen (LS, gemeint sind die analogen Serious Games) dauert jede Station lediglich 15 Minuten und beinhaltet u. a. jeweils ein sogenanntes „Minigame“, das üblicherweise „mit den anderen Games und den Briefings für die Moderierenden in einen handelsüblichen Koffer passt. Moderiert wird stets von Kolleginnen und Kollegen auf Basis eines Train-the-Trainer-Konzepts“ [30].

„Eine LS setzt Kommunikationsziele auf mehreren Ebenen um. Es handelt sich um eine Clip-artige Vermittlung von Wissen in Form einer Simulation. Die Teilnehmenden sollen über das Thema Sicherheit ins Gespräch kommen, d. h. ihr Wissen und ihre persönlichen Erfahrungen einbringen. Hierdurch soll eine Integration von Emotionen in die Diskussion erfolgen, um das (…) beschriebene Zusammenspiel von ‚Wissen – Wollen – Können´ für ein nachhaltiges Bewusstsein zu initiieren. Die Zielgruppen einer LS sind, ebenso wie die vermittelten Inhalte, generisch zu verstehen und unterliegen somit keiner spezifischen Ordnung. Die zu vermittelnden Inhalte werden abstrakt dargestellt und eignen sich so für jeden Aufnahmehorizont (…) Ziel der Kommunikation ist die Veränderung der Wahrnehmung, der Einstellung und des Verhaltens der Zielgruppen eines Unternehmens.“ [31]

LS bieten diverse Vorteile gegenüber herkömmlichen Schulungsformaten:

- Nutzung als Teaser, „um weitere Wissensbedarfe bei den Teilnehmer/-innen zu sicherheitsrelevanten Fragen zu erzeugen und somit innerhalb einer Sicherheitskommunikationskampagne als entscheidender Baustein zu dienen“ [31].
- Incentivierung mit Punkten pro Spiel bei verzahnten Trainingsevents mit infolge von Synchronisierung zeitgleich ablaufenden Stationen, um den Wettbewerbscharakter und die Motivation innerhalb der Teams zu steigern.
- Leichte Adaption an die Bedürfnisse der anwendenden Organisation mit bedarfsweiser Weiterentwicklung.
- Aspekt „Talking Security“ als Nachhaltigkeitsfaktor, d. h. der „diskursive Effekt des Formates führt zu einer Kommunikation unter den Teilnehmenden auch über Sicherheitsfragen hinaus und fördert so den gegenseitigen Austausch und das Team Building“ [31]. Außerdem sprechen die Teilnehmenden nach „Absolvierung der Stationen über die dort erlebten Themen sowie das Format selbst“ [31].

LS können potenziell „auch bei Organisationen mit gering entwickeltem Reifegrad zum Schulungs-Thema angewendet werden“ [31].

Die LS sind primär für eine Übernahme von Unternehmen im Rahmen eines Train-the-Trainer-Ansatzes erstellt worden, d. h. die nutzenden Organisationen selbst planen und realisieren inhouse miteinander verzahnte Trainingsevents von z. B. vier LS à 15 Minuten (gesamt demnach eine Stunde), die synchron mit Teams von bis zu 12 Personen von eigenen Mitarbeiter/-innen moderiert werden. Auf diese Weise können in 60 Minuten bis zu 48 Teilnehmende per LS sensibilisiert werden. Bei bis zu fünf Wiederholungen sind am Tag rechnerisch maximal 288 Teilnehmende möglich, mithin eine größere Anzahl als die KMU-Definition in Bezug auf Mitarbeiterdimension vorgibt. Jedoch liegt die „ideale Zahl (…) zwischen sechs und acht Teilnehmer/-innen je Team und Station. Hierdurch wird die Sicht aller auf das Spielfeld sowie die Diskussion untereinander gewährleistet. Zudem kann der Moderierende zeitgerecht auf Fragen eingehen und die Diskussion bei Bedarf leiten oder neu anstoßen. Die Teilnehmenden sind für ihn jederzeit sichtbar und können sich dem stattfindenden Diskurs nicht absichtlich entziehen bzw. diesem im Menschengedränge entzogen werden“ [31].

Die Moderation läuft in drei Stufen ab:

- LS-Briefing mit Vorstellung von Moderation und Thema, Abfragen von Erfahrungen in Bezug auf das jeweilige LS-Thema mit Team-Diskussion
- LS-Spiel (Simulation, im Rahmen der „Security Arena“ in der Regel „Minigame“ genannt)
- LS-Debriefing mit Auflösung der Spiel-Aufgabe und Klärung offener Fragen, die während der Spielsituation entstanden sind

„Der Moderierende stellt zu Beginn das Thema vor und leitet mit Fragen nach eigenen Erfahrungen und Meinungen der Teilnehmenden zu den Inhalten ein. Auch Fragen nach der eigenen Wahrnehmung der Sicherheitsorganisation im Unternehmen können gestellt werden. Der im Zuge der Entwicklung der Station entstandene Moderationsleitfa-

Abb. 12 und 13: *Analoges Serious Game 3.3.3*

den dient dem Moderierenden dabei als Hilfestellung, ist jedoch keine strikt abzuarbeitende Checkliste. Vielmehr liegt es in seinem Ermessen, den Fortgang dieser 15 Minuten zu gestalten. Seine Authentizität und Performance sind also ein wesentlicher Faktor und entscheiden über das Gelingen der LS für die Teilnehmenden. Neben ausgeprägten kommunikativen Eigenschaften muss der Moderierende zudem in der Lage sein, schwierige Charaktere unter den Teilnehmenden und die mit ihnen einhergehenden Stimmungen zu antizipieren, aufzufangen und bestenfalls in die Diskussion innerhalb der Gruppe zu integrieren. Dies gilt auch für konträre Meinungen zum Thema. Der bzw. die Moderierende schließt die Station mit einem Debriefing ab und räumt, soweit angemessen, Zeit für Fragen seitens der Gruppe ein. Sollte eine Station früher beendet sein und keine weiteren Fragen zur Klärung bestehen, hält der bzw. die Moderierende die Gruppe an der Station, um eine Störung der anderen Stationen und Gruppen durch einen frühzeitigen Wechsel zu unterbinden." [31]

Als ein Nachteil in Bezug auf eine vertiefende Sensibilisierung könnte die relativ kurze Dauer einer klassischen LS mit 15 Minuten Dauer betrachtet werden. „Durch den mangelnden Raum für Details ersetzt eine solche Station kein Intensivtraining, in dem die Durchdringung der Inhalte für alle Teilnehmenden nachvollzogen werden kann. Zudem müssen aus Gründen der Akzeptanz des Formats und der Kostenfrage meist interne Beschäftigte als Moderierende für die Stationen gewonnen werden." [31]

Sämtliche LS bzw. analoge Serious Games des Projektes „ALARM Informationssicherheit" sind jedoch zeitlich skalierbar, d. h. die o. g. 15 Minuten als Richtwert ließen sich auch auf 20, 30 Minuten ausdehnen, die Moderationsbriefings lassen in Bezug auf die Quantität der Inhalte sogar eine zeitliche Erweiterung und damit Nutzung innerhalb von Langtrainings mit bis zu 60 Minuten zu, wenn es sich nicht um synchrone Trainings bzw. miteinander verzahnte LS handelt.

„Im Gegensatz zur Online-Sensibilisierung mithilfe eines WBTs (Web Based Training), das bei aller Selbstbestimmtheit relativ ‚einsam' stattfindet, hebt z. B. die Security Arena Awareness von der kognitiven Ebene der Informationsvermittlung auf die für das Lernen so wichtige Beziehungsebene. Der/die Einzelne profitiert dabei von der emotionalen Aufladung innerhalb der Gruppe. Denn soziale Teilhabe führt zu Involvement, mehr Lebendigkeit und zu einer ganzheitlichen Awareness, bei der einzelne Lernschritte vor allem über die Interaktion mit Erlebnissen belegt werden und auf diesem Weg (diskursives Lernen) eine bessere Resilienz und Memorierbarkeit erzielt werden. D. h. die Security Arena bildet Gesprächsthemen und bringt Sicherheit nach dem Prinzip ‚Talking Security' in einen permanenten kommunikativen Umsatz." [32]

LS bilden in ihrer Ausschließlichkeit kein probates Medium hinsichtlich einer dauerhaft wirksamen Security Awareness. Eine nachhaltige Kampagne kann im Mix mit weiteren Medien und Kanälen und bei ausreichender Zielgruppendiversifikation unter Berücksichtigung geeigneter psychologischer Verfassungen erfolgen. LS sind aufgrund der Kürze und hohen Sichtbarkeit innerhalb der Organisation ein idealer Teaser für einen Kampagnen-Kickoff – auch weil hierüber unter den Teilnehmer/-innen potenziell Bedarfe für weitere Maßnahmen geschaffen werden. D. h. die/der ideale Mitarbeiter/-in bildet für sich Fragen, deren Beantwortung den Bedarf nach weiteren Awareness-Maßnahmen erzeugen. Über die Empfehlung, sich vertiefend mit Inhalten in weiteren Kanälen und Formaten zu beschäftigen, werden im Sinne einer integrierten Kommunikation auch weitere Awareness-Maßnahmen implizit beworben.

3.2 Typischer Ablauf eines analogen Lernszenarios

Die Moderationsbriefings der analogen Lernszenarien gehen ein auf folgende Aspekte und sind auch in dieser Reihenfolge angeordnet:

- Material
- Spielvorbereitung
- Ziel (didaktische Intention)
- Story/Spieldynamik
- Moderation
- Goldene Regeln
- Mögliche Fragen für die Moderation
- Lösung

Die analogen Serious Games des Projektes „ALARM Informationssicherheit" sind mit Moderationsanleitungen ausgestattet, so dass eine für Informationssicherheit zuständige Person die Moderation übernehmen kann. Da sie als Lernstationen angelegt sind, ist die damit verbundene Spieldauer skalierbar, so dass sie von 15 Minuten bis zu einer Stunde Lernmaterial bieten [33].

In der Materialliste ist beschrieben, was Sie benötigen. Neben dem originären Material für das jeweilige Serious Game wird vorausgesetzt, dass Sie die notwendige Tischfläche zur Anordnung der Materialien sowie ein Smartphone als Stoppuhr bereitstellen. Bei den Goldenen Regeln und den Fragen sind – je nach Thema und Umfang – jeweils je 6-10 allgemeingültige Regeln zur Risikovermeidung und Prävention benannt und bis zu 25 Fragen, die aus einem Mix aus Wissens- und Meinungsfragen, projektiven Fragen und Anregungen zur Story- bzw. Metaphernsuche (Imagination) bzw. zu Rollenwechsel oder- spielen bestehen. Aus diesem Angebot können sich Moderatoren/-innen entsprechend ihren persönlichen Wissenstands und ihrer sonstigen Fähigkeiten bzw. den Fähigkeiten der Zielgruppen bzw. Vertiefungsintention bedienen (s. auch Kapitel 4.3).

Die Moderation gliedert sich stets in 3 Teile, Einleitung (Willkommen bzw. Briefing), Spiel und Nachbereitung (Lösung mit Debriefing und Verabschiedung), etwa in dieser Form:

Abb. 14 und 15: *Analoges Serious Game 3.3.4*

Schritt 1: Einleitung (ca. 3-6 Min.)

- Stellen Sie sich und das Thema dieser Station kurz vor.
- Fragen Sie innerhalb des Teams ab, wer mit dem Thema bereits in Berührung kam und ob man in diesem Kontext bereits mit Sicherheitsproblemen konfrontiert war.
- Welcher Art waren diese Probleme? Gab es Lösungen und wenn ja, wer oder was hat dabei geholfen?
- Lassen Sie sich die Vorfälle als Geschichte erzählen. Was ist passiert – mit welchen konkreten Folgen?
- Goldene Regeln und Fragen können gerne an den passenden Stellen eingestreut und behandelt werden.

Schritt 2: Spiel (5-8 Min.)

- Erklären Sie die Regeln des Spiels und welche Punktzahl erwartet werden kann.
- Arrangieren Sie alle für das Spiel benötigten Materialien und starten Sie das Spiel.
- Gegebenenfalls geraten die Teams nicht in Zeitnot, wenn sie paarweise oder in Kleingruppen vorgehen (Karten entsprechend auf z. B. Kleingruppen verteilen, die synchron vorgehen).

Schritt 3: Nachbesprechung (ca. 3-6 Min.)

- Beenden Sie das Spiel, addieren Sie die Punkte und bieten Sie eine kurze Nachbesprechung an, bei der Sie offene Fragen, die im Verlauf des Spiels entstanden sind, klären können.
- Es ist wichtig, das Material (z. B. Spielkarten) direkt nach Beendigung wieder zu durchmischen, bevor die nachfolgende Gruppe eintrifft.
- Fragen und Antworten zur Vorbereitung, Durchführung, Moderation und Nachbereitung finden Sie in einem FAQ in Kapitel 4

3.3 Übersicht analoger Serious Games

Die Themen der entwickelten Serious Games ergeben sich aus den Ergebnissen bzw. einem Ranking der KMU-Grundlagenstudie [11]. 4 der finalen 7 Serious Games wurden über die 2. Wirkungsanalyse [29] im Projekt „ALARM Informationssicherheit“ getestet. Bei zwei Themen (3.2.6 und 3.2.7) wurde das Minigame ausgetauscht. Ein Serious Game (3.2.2, vormals „Kundendaten sicher managen in der Cloud“) wurden nach dieser 2. Studie aufgrund der Testergebnisse durch das Thema „Multifaktor-Authentisierung“) ersetzt. Diese 3 Serious Games wurden anschließend neu pilotiert und dabei weiteren Tests unterzogen, jedoch ohne die tiefenpsychologische Ebene zu evaluieren.

Folgende Serious Games wurden entwickelt:

- Sicher zuhause wohnen & arbeiten
- Multifaktor-Authentifizierung.
- Die 5 Phasen des CEO Fraud
- Mobile Kommunikation, Apps & Co.
- Cyber Pairs
- Infoklassen-Roulette
- Daten- und Informationsschutz

3.3.1 Sicher zuhause wohnen & arbeiten

Das Spiel besteht aus:

- 1 Spielfeld (168 cm x 118 cm), das ein größeres Einfamilienhaus als Lernkarte zeigt
- 17 orange Risikokarten (DIN B-7)
- 17 grüne Schutzkarten (A-Q, DIN B-7)
- Moderationsblätter mit Lösung

Im Rahmen dieses Serious Game sehen wir auf dem Spielfeld-Wimmelbild ein Haus, in dem zwei befreundete Paare mit ihren Kindern und in einem Fall auch mit dem (Groß-) Vater leben und arbeiten. Ihrem Wirken sind 17 Szenarien zugeordnet, die jeweils ein Informationssicherheits- oder ein Datenschutz-Risiko beinhalten. Die Risiken sind auf 17 orangen Risikokarten beschrieben, entsprechende Schutzmaßnahmen auf 17 grünen Schutzkarten. Es sollen zunächst in einem ersten Durchgang die orangen Risikokarten auf die entsprechenden Szenarien abgelegt werden und in einem zweiten Durchgang die grünen Schutzkarten auf die passenden Risiken.

- Didaktische Intention: Risiken und deren Präventionsmaßnahmen im Homeoffice bzw. Zuhause erkennen und adäquat darauf reagieren, um Risiken bzw. deren potenzielle Wirkung zu mindern
- Geplante Nettospielzeit: 2 x 2,5 Minuten (gesamt 5 Minuten)
- Maximale Punktzahl: 34
- Potenzielle Zielgruppe: alle, die im Homeoffice wirken

3.3.2 Multifaktor-Authentifizierung

Das Spiel besteht aus:

- 1 Spielfeld (100 cm x 80 cm), das 20 nummerierte Sortierfelder für Passwörter abbildet
- 20 Spielkarten (DIN A6) mit 20 verschiedenen Passwortphrasen, einem Buchstabencode zum schnelleren Identifizieren und einem zusätzlichen Zifferncode für Teil zwei des Serious Games
- 2 Boxen, davon 1 große mit Zahlenschloss, 1 kleinere mit Schlüsselschloss (die beiden Boxen passen nicht in die Standard-Umverpackung dieser Station)
- 12 Schlüssel (davon 10 falsche) für die kleine Box
- 12 transparente Dokumententaschen
- 1 Tisch (etwa 120 cm x 80 cm)
- Moderationsblätter mit Lösung

Dieses Serious Game besteht aus mehreren Teilen und folgt der Logik von Escape Games. Zunächst sollen die 20 Passwortkarten entsprechend der jeweiligen Stärke geranked werden, indem sie auf den 20 Feldern des Spielfeldes

Abb. 16: *Analoges Serious Game 3.3.5*

in der richtigen Reihenfolge von 1–20 verteilt werden. Die Ziffern-Codes der Top-3-Karten ergeben in der richtigen Reihenfolge des „Stärke"-Rankings den passenden Zahlencode für die große Box, d. h. mit diesem dreistelligen Code lässt sich das Zahlenschloss öffnen. In der großen Box befindet sich eine kleine Box mit einem Schloss, zu der der zugehörige Schlüssel gefunden (Dokumententasche!) und zur Anwendung gebracht werden soll. Ist die kleine Box geöffnet, in der man z. B. auch ein Incentive „verstekken" kann, ist diese Übung beendet.

- Didaktische Intention: Es soll vom Thema Passwortschutz mit dem Hauptaspekt „starke Passwörter" in das Thema MFA hineingeführt werden, u. a. mit der Kernbotschaft, dass ein Faktor wie z. B. das Passwort alleine nicht mehr ausreichend ist, um Anwendungen bzw. Daten zu schützen.
- Geplante Nettospielzeit: 6 Minuten in drei Teilen
- Maximale Punktzahl: 30
- Potenzielle Zielgruppe: alle

3.3.3 Die 5 Phasen des CEO Fraud

Das Spiel besteht aus:

- 1 Spielfeld (120 x 120 cm), das im Zentrum
- 22 Anlegefelder hinsichtlich der 5 Phasen eines typischen CEO Fraud sowie wissenswerte Informationen („Good-to-know") zum Thema im Stil einer Infografik an den Rändern abbildet
- 31 Spielkarten, d. h. 25 CEO Fraud-Prozesskarten (7 x 7 cm), davon 22 „richtige" und 3 „falsche", sowie 6 E-Mail-Karten (DIN A5), davon 4 Phishing-E-Mails, die zur Vorbereitung eines CEO Fraud im Sinne von Spear Phishing eingesetzt werden, und 2 unkritische E-Mail-Karten (kein Phishing, d. h. ohne jede Betrugsabsicht)
- Moderationsblätter mit Lösung

22 Spielkarten sollen auf dem Spielfeld in der richtigen Prozessreihenfolge eines CEO Fraud sortiert werden. Die 3 „falschen" Karten, die nicht in diesen Prozess passen, werden aussortiert. Optional sollen in einem Teil 2 des Spiels aus den 6 E-Mail-Karten die 4 ausgesucht und im Zentrum des Spielfelds platziert werden, die mithilfe von Phishing CEO Fraud einleiten bzw. Betrug unterstützen. Dafür ist nach typischen Phishing-Hinweisen zu suchen.

- Didaktische Intention: Risiken und deren Präventionsmaßnahmen im Kontext CEO Fraud und den damit verbundenen Kollateralrisiken, z. B. Spear Phishing, erkennen und adäquat darauf reagieren
- Geplante Nettospielzeit: 6 Minuten
- Maximale Punktzahl: 31
- Potenzielle Zielgruppe: Mitarbeiter/-innen der Finanzbuchhaltung, des Controllings und der HR-Abteilung, Management und andere Führungskräfte

3.3.4 Mobile Kommunikation, Apps & Co.

Das Spiel besteht aus:

- 1 Spielfeld (168 cm x 118 cm)
- 12 orange Risikokarten (DIN B-7)
- 12 grüne Schutzkarten (A-L, DIN B-7)
- Moderationsblätter mit Lösung

Hier ist auf dem Spielfeld eine Lernkarte mit einem Wimmelbild abgebildet, das 12 Szenarien bei der Smartphone- bzw. App-Nutzung zeigt. Dafür werden drei Etagen eines U-Bahnhofs und ein Haus im Hintergrund mit verschiedenen Personen als zentrales Key Visual abgebildet. Zusätzlich befinden sich an den Rändern vergrößerte Abbildungen der von den jeweiligen Personen benutzten Smartphones – jeweils mit den Szenarien zugehörigen Screenshots.

Den 12 nummerierten Szenarien und 12 ebenfalls nummerierten und zu den Szenarien im U-Bahnhof bzw. Haus passenden Smartphones sind 12 Informationssicherheits- bzw. Datenschutz-Risiken zugeordnet. Die Risiken sind auf 12 orangen Risikokarten beschrieben, entsprechende Schutzmaßnahmen auf 12 grünen Schutzkarten. Es sollen wie im Serious Game unter 3.2.1 zunächst in einem ersten Durchgang die orangen Risikokarten auf den hellen, transparenten Feldern an den entsprechenden Szenarien abgelegt werden und in einem zweiten Durchgang die grünen Schutzkarten auf die passenden Risiken.

- Didaktische Intention: Risiken und deren Präventionsmaßnahmen im Kontext mobiler Kommunikation bzw. App-Nutzung erkennen und adäquat darauf reagieren, Zugriffsrechte von Apps aktiv einschränken
- Geplante Nettospielzeit: 2 x 2,5 Minuten (gesamt 5 Minuten)
- Maximale Punktzahl bei Incentivierung: 24
- Potenzielle Zielgruppe: alle

3.3.5 Cyber Pairs

Das Spiel besteht aus:

- 32 blaue Cyber-Memokarten (7x7 cm, Ziffern-Codes: #1-32)
- 16 orange Cyber-Risikokarten (7x7 cm, Großbuchstaben-Codes: #A-P)
- 16 grüne Cyber-Schutzkarten (7x7 cm, Kleinbuchstaben-Codes: #a-p)
- Moderationsblätter mit Lösung

Es sollen zunächst in einem ersten Durchgang die 32 blauen Cyber-Memokarten so arrangiert werden, dass 16 korrekte Cyber-Security-Begriffe (i. e. S. Angriffsvektoren) entstehen, z. B. nebeneinander in 2 Spalten, jeweils mit Platz für 2 weitere Karten rechts bzw. links neben den beiden blauen Paaren. In einem zweiten Durchgang sollen den 16 Begriffen die 16 orangen Cyber-Risikokarten passend zugeordnet und neben den blauen Cyber-Memokarten

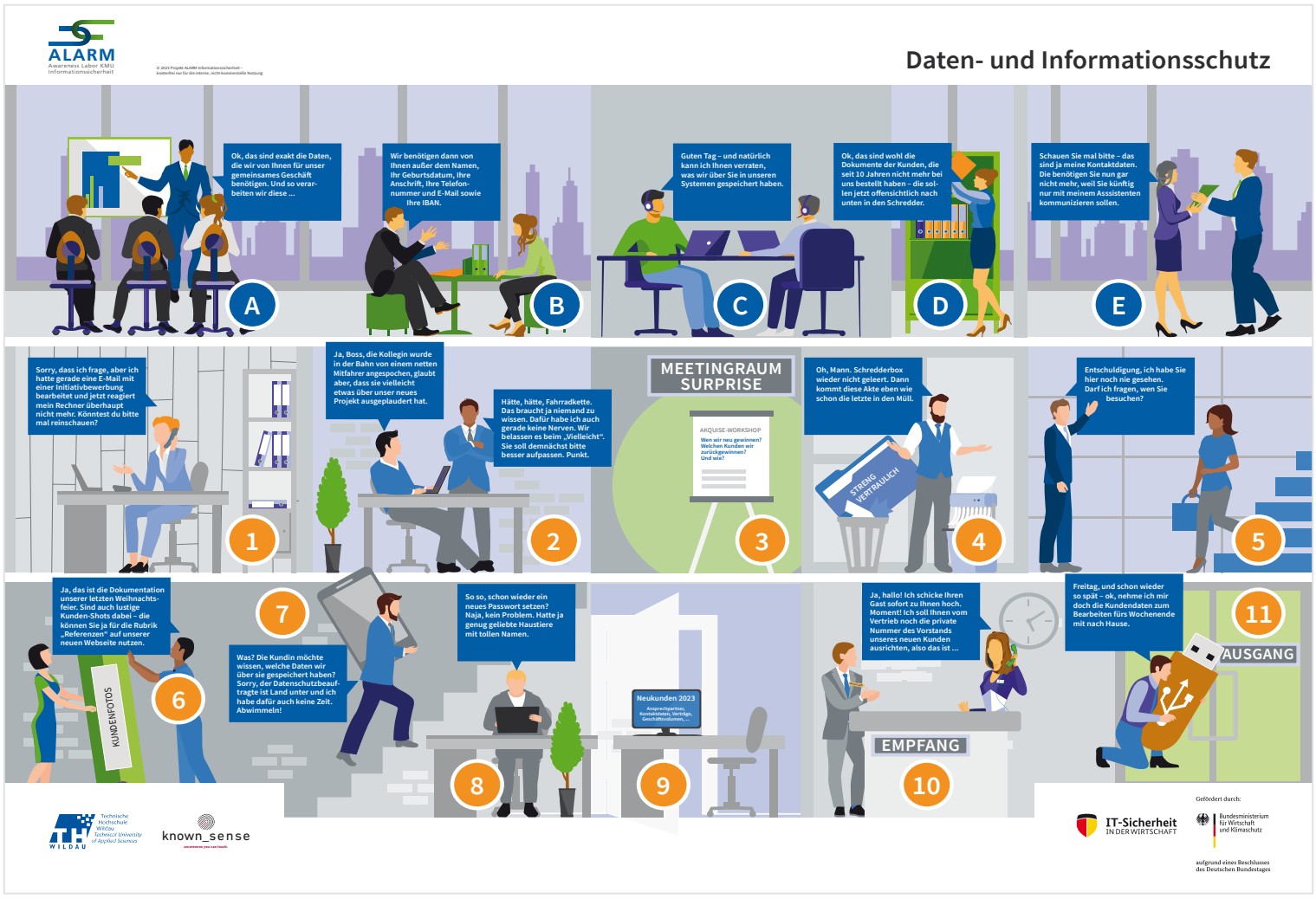


Abb. 17 und 18: *Analoge Serious Games 3.3.6 (Spielfeld und Auszug Spielkarten oben) und 3.3.7 (Spielfeld unten)*

abgelegt werden. In einem dritten Durchgang sollen die 16 grünen Cyber-Schutzkarten passend neben den orangen Cyber-Risikokarten abgelegt werden. Die orangen und grünen Karten sind jeweils beidseitig bedruckt, d. h. auf den Vorderseiten befinden sich Definition und Präventionsmaßnahmen in Kurzform, auf den Rückseiten werden die Teaser der Vorderseite ausführlicher erklärt.

- Didaktische Intention: Risiken und deren Präventionsmaßnahmen im Kontext Cyber Security und digitaler Schattenwirtschaft, insbesondere bei der Verwendung diverser Social Engineering-Methoden, erkennen und adäquat darauf reagieren, Motive des bzw. das Begriffsfeld „Cyber Security" verstehen, um singuläre Phänomene als ein „Big Picture" ganzheitlich betrachten zu können
- Geplante Nettospielzeit: 3 x 2 Minuten (gesamt 6 Minuten)
- Maximale Punktzahl: 48
- Potenzielle Zielgruppe: alle

3.3.6 Infoklassen-Roulette

Das Spiel besteht aus:

- 1 Spielfeld (70 cm x 100 cm)
- 36 Spielkarten (DIN A6) in sechs verschiedenen Kategorien
- 1 Roulettekessel mit zwei Kugeln (oder online unter https://diz.wildau.biz/roulette/index.html den digitalen Roulettekessel nutzen)
- 1 Rateau
- 100 Jetons (je 20 x 5, 10, 20, 50, 100)
- Moderationsblätter mit Lösung

Dieses Serious Game vereint Elemente aus Roulette mit Inhalten zum Thema Informationsklassifizierung bzw. Schutzziele. Über das Drehen eines Roulette-Rads wird entschieden, aus welcher der 6 Kategorien (Informationsklassifizierung allgemein, Schutzziele der Informationssicherheit, Bedeutung der Schutzklassen, Auswirkungen von Schutzverletzungen, Schutz von Kundeninformationen bzw. personenbezogenen Daten, Auszeichnen von bzw. Umgang mit Dokumenten und Informationen) eine Karte gezogen werden soll. Die Grundaussage bzw. Kernbotschaft der jeweiligen Mini-Storys auf den gezogenen Karten muss mit „richtig" oder „falsch" beurteilt werden, indem die zugeteilten Jetons in dem Spielfeld auf „RICHTIG" oder „FALSCH" gesetzt werden. Über klassisches „Zocken" auf die Inhalte kann somit der Gesamtwert der jeweils eigenen Jeton-Portfolios erhöht werden, um möglichst viele Punkte zu erreichen.

- Didaktische Intention: Schutzbedarf von Informationen kennen und entsprechend des jeweiligen Risikos klassifizieren können, Verwendungszwecke differenziert betrachten
- Geplante Nettospielzeit: 8 Minuten
- Maximale Punktzahl: je nach Anzahl von Teams 30
- Potenzielle Zielgruppe: alle, die mit sensitiven Informationen umgehen

3.3.7 Daten- und Informationsschutz

Das Spiel besteht aus:

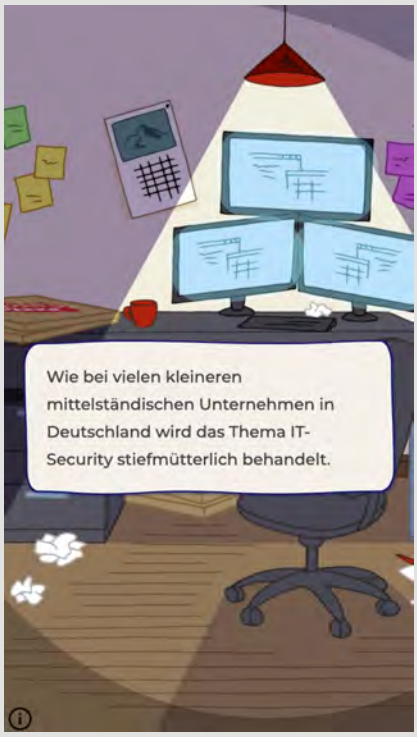
- 1 Spielfeld (168 cm x 120 cm)
- 16 Spielkarten (11,8 cm x 8,4 cm), davon 5 blaue Spielkarten #1–5 (Rechte der Kunden/-innen) und 11 grüne Spielkarten #A–K (Präventionsstrategien, z. B. Schutz von Mitarbeitenden- bzw. Kundendaten)
- 15 „Bilderrahmen"-Karten #1–15 (6 x 8 cm, personenbezogene Daten)
- Moderationsblätter mit Lösung

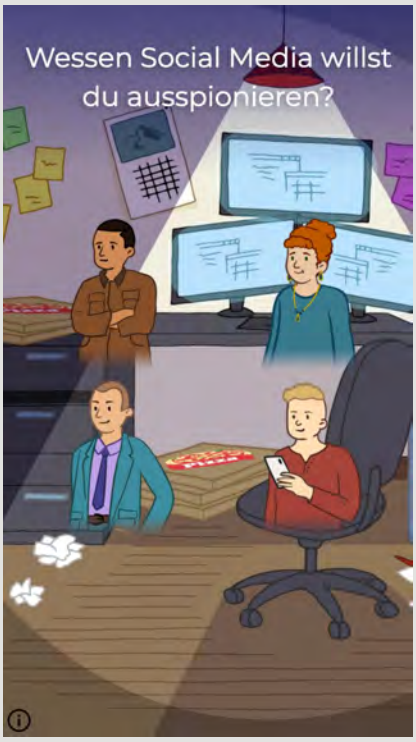
Dieses Serious Game vereint Risiken und Präventionsstrategien aus Daten- und Informationsschutz. Auch hier wird mit dem bewährten Ansatz eines Wimmelbild-Spielfelds gearbeitet. Darauf sehen wir das Innere eines typischen Bürogebäudes und Mitarbeiter/-innen bei der Erledigung ihrer Aufgaben und 16 Szenarien auf drei Ebenen. Auf der obersten Ebene sind Rechte von Kunden/-innen dargestellt, auf der 2. und 3. Ebene 11 Szenarien, die jeweils ein Informationssicherheits- oder ein Datenschutzrisiko beinhalten. Es sollen zunächst in einem ersten Durchgang alle 16 hierzu gehörigen Spielkarten auf dem Spielfeld so arrangiert werden, dass sie zu den dargestellten Szenarien passen. Optional können in einem zweiten Spielteil die so genannten „Bilderrahmen"-Karten ins Spiel gebracht werden, um die Unterscheidung von personenbezogenen und nicht-personenbezogenen Daten zu simulieren. Dafür werden diejenigen Karten, die KEINE personenbezogenen Daten umfassen, dort an den Wänden der auf dem Spielfeld dargestellten Büros platziert, wo ausreichend Platz ist – diese Karten werden mithin wie Bilder „aufgehängt".

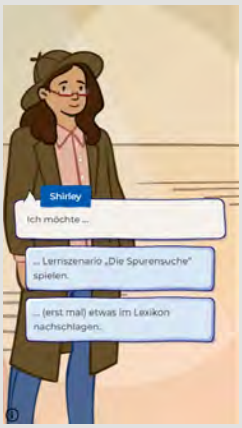
- Didaktische Intention: Dieses Serious Game soll dabei unterstützen, Daten- und Informationsschutz insbesondere bei Kunden/-innen zu gewährleisten, indem der Umgang mit den wichtigsten Risiken und Schutzstrategien rekapituliert bzw. eingeübt wird.
- Geplante Nettospielzeit: 4 Minuten + optional 2 Minuten durch Teil 2 (gesamt 6 Minuten)
- Maximale Punktzahl: 22
- Potenzielle Zielgruppe: alle, die mit sensitiven Informationen umgehen

3.4 Verzahnung mit den digitalen Serious Games des Projektes „ALARM Informationssicherheit"

Bei den 7 digitalen Serious Games handelt es sich um immersive Geschichten, die Alltagssituationen aus dem Berufsleben in KMU darstellen [34]. In Kombination mit







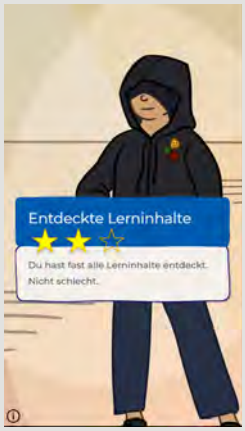


Abb. 19 bis 27: *Digitale Serious Games 3.4.1 bis 3.4.3 (von oben nach unten rechts)*

einer auditiven und visuellen Ansprache ermöglichen sie das Eintauchen der Spielenden in die Situationen, so dass die Spielenden Bezüge zu ihrem Arbeitsalltag herstellen können [35]. Dabei behandelt jedes Serious Game ein anderes für KMU informationssicherheitsrelevantes Schwerpunktthema. 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 und die Spielenden begegnen immer wieder denselben Personen.

Die digitalen Serious Games können als Vertiefung und Ergänzung zu den analogen eingesetzt werden oder unabhängig von diesen. Die Mischung von analogen und digitalen Serious Games verfolgt einen ganzheitlichen Ansatz im Kanalmix, führt zu Abwechslung und wirkt auf Teilnehmende potenziell belebend und motivierend. Der Vorteil gegenüber dem oben beschriebenen analogen Ansatz: Mitarbeiter/-innen können die Games, deren Themen sie interessieren, unabhängig von Zeit, Ort und Unterstützung- z. B. durch Moderierende, spielen [33], so dass Moderation und gegebenenfalls Verknüpfung mehrerer Stationen zu einem organisierten Trainingsevent wegfallen. Dafür fehlen die wichtigen diskursiven Anteile, es sei denn, die Organisation bietet eine gemeinsame, moderierte Nachbetrachtung des Erlebten bei den digitalen Games an – dies wird von der TH Wildau zwar explizit empfohlen, dürfte jedoch vermutlich in den Arbeitsalltag unrealistisch zu implementieren sein. Allenfalls wäre vorstellbar, dass z. B. während eines analogen Events auf Inhalte bereits durchgespielter digitaler Serious Games eingegangen wird.

Die einzelnen Spiele im Überblick:

3.4.1 Der erste Tag – Social Engineering & Passwortschutz

- Didaktische Intention: Ziel des Spiels ist: eine Einführung in das Thema Informationssicherheit anhand klassischer Situationen rund um Social Engineering und Passwortschutz, die eine hohe Identifikation für alle bieten.
- Wertung: Bewertet werden generelles Sicherheitsverständnis und Sozialkompetenz.
- Passung analoges Serious Game: alle mit Fokus auf Multifaktor-Authentifizierung, Die 5 Phasen des CEO Fraud, Cyber Pairs

3.4.2 Der Hackerangriff – Social-Engineering-Methoden & -Werkzeuge

- Didaktische Intention: Ziel des Spiels ist es, die gängigen, von Hackenden benutzten Strategien, in einer reellen Situation und aus der Perspektive der Hackenden kennenzulernen und dabei spielerisch zu erleben, wie schon kleinste Sicherheitslücken ausreichen, um Hackenden den Zugriff zu erlauben.
- Wertung: Bewertet werden Effizienz und die Variabilität an Angriffswegen, die die Spielenden ausprobieren.
- Passung analoges Serious Game: Die 5 Phasen des CEO Fraud, Cyber Pairs

3.4.3 Die Spurensuche – CEO-Fraud-Methoden & -Schutzmaßnahmen

- Didaktische Intention: Ziel des Spiels ist, gängige Praktiken von CEO Fraud aufzudecken und wirksame Schutzmaßnahmen zu ergreifen. Eine besondere Rolle spielt bei diesem Thema die Zeit – nur wenn die Spielenden die Attacke rechtzeitig auflösen, können sie größeren Schaden verhindern.
- Wertung: Bewertet werden Effizienz, entdeckte Lerninhalte und Sozialkompetenz.
- Passung analoges Serious Game: Die 5 Phasen des CEO Fraud

3.4.4 KI im Homeoffice – Schutzmaßnahmen im Homeoffice & Smart Home

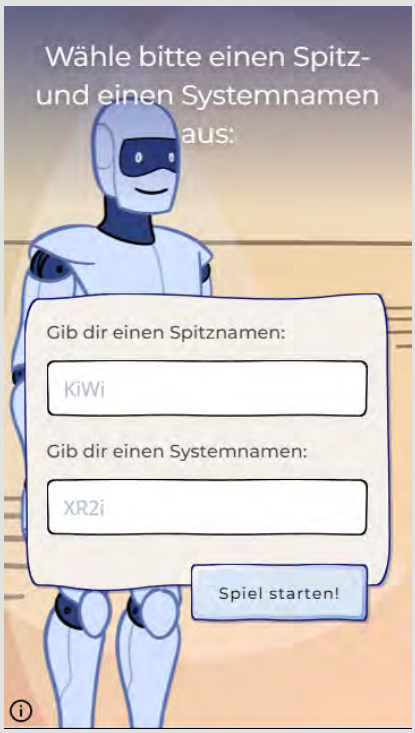
- Didaktische Intention: Ziel des Spiels ist es, nicht einen großen Aktionserfolg zu erzielen, sondern durch kleinere Aufgaben die beliebtesten Fehler im Homeoffice zu finden. Dabei wird in praktischen und witzigen Beispielen auf die Tücken des Homeoffice aufmerksam gemacht.
- Wertung: Bewertet werden dabei Sicherheitsbewusstsein und Machine Learning.
- Passung analoges Serious Game: Sicher zuhause wohnen & arbeiten

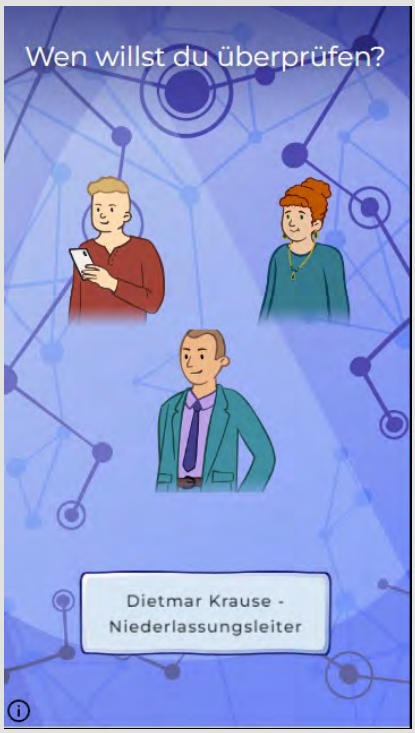
3.4.5 Alles nur geCLOUD – Password-Hacking-Methoden & Passwortschutz

- Didaktische Intention: Das Thema Datenspeicherung in der Cloud und Passwortsicherheit soll aus zwei verschiedenen Perspektiven beleuchtet werden, des Angreifenden und des Aufklärenden. Dabei stehen jeweils unterschiedliche Aspekte der Gefährdung im Mittelpunkt und erlauben ein ganzheitliches Erleben des Themas.
- Wertung: Bewertet werden Effizienz und Gründlichkeit im Sinne eines planvollen, jederzeit reflektierten Wirkens.
- Passung analoges Serious Game: Multifaktor-Authentifizierung

3.4.6 Eine Klassifizierung für sich – Info-Klassen und Verwendungszweck

- Didaktische Intention: Ziel des Spiels ist es, ein System zu entwickeln, wie Informationen richtig





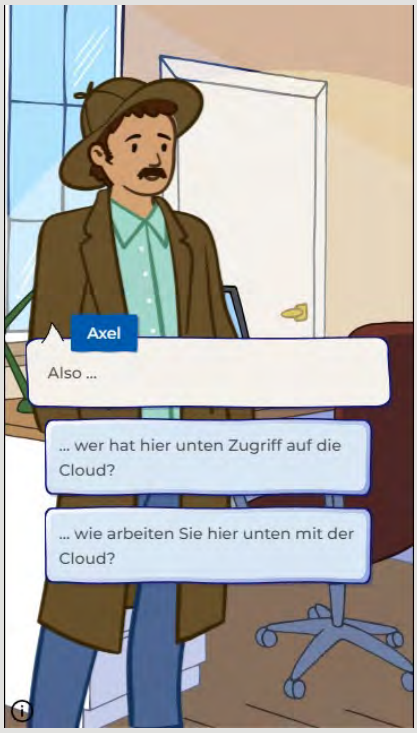


Abb. 28 bis 33: *Digitale Serious Games 3.4.4 und 3.4.5 (von oben nach unten)*

klassifiziert werden können. Dabei gibt es drei Informationskategorien, denen bestimmte Eigenschaften zugeordnet werden.

- Wertung: Bewertet werden dabei die Fähigkeit, Kategorien zu definieren, Informationen einzuordnen, Termine zu verwalten und Fehler zu identifizieren.
- Passung analoges Serious Game: Infoklassen-Roulette

3.4.7 Der Ransomware-Angriff – Verschlüsselung und Messenger-Dienste

- Didaktische Intention: Ziel des Spiels ist es, die Sicherheitslücke im Messenger zu identifizieren und unter Zeitdruck ein verschlüsseltes Passwort zu entschlüsseln, um die gefährdeten Daten zu sichern.
- Wertung: Bewertet werden Codeknacker Kompetenz und Aufmerksamkeit.
- Passung analoges Serious Game: Mobile Kommunikation, Apps & Co, CEO Fraud, Cyber Pairs

3.4.8 Ziel der digitalen Serious Games und Spieldynamik

In den digitalen Serious Games können Mitarbeiter/innen die Themen der analogen Serious Games vertiefen und mit anderen Schwerpunkten erleben. Die digitalen Serious Games können aber auch unabhängig von den analogen oder alternativ auch vor diesen absolviert werden.

In jedem digitalen Serious Game nehmen die Spielenden wechselnde Rollen ein – z. B. handeln sie als Sicherheitsfachkräfte, Hackende, Ermittelnde oder Künstliche Intelligenz. So lernen sie die komplexen Themenwelten aus verschiedenen Blickwinkeln kennen und verstehen. Die Teilnehmenden treffen also in kurzen Rhythmen Entscheidungen und bestimmen dadurch den weiteren Verlauf der Geschichte. Mit jeder Entscheidung begeben sie sich auf ihre ganz persönliche Lernreise, die von ihrem Wissen und ihren Präferenzen bestimmt wird. Jedes Serious Game enthält zwei bis drei Lernpfade, die die Spielenden durch ihre Entscheidungen einschlagen. Am Ende jedes Spiels erhalten die Teilnehmenden Feedback zu den erzielten Punkten. Dieses beinhaltet Vorschläge und Aufforderungen an die Spielenden sowie eine kurze Zusammenfassung über die im konkreten Spiel gewonnenen Erkenntnisse (lessons learned). Auch bereits im Laufe des Spiels werden Nachrichten eingeblendet, die auf vorteilhafte oder nachteilige Entscheidungen und Verhaltensweisen aufmerksam machen. Zudem bietet ein Lexikonmodul die Möglichkeit, wichtige Begriffe der Informationssicherheit vor und nach dem Spiel nachzulesen.

3.5 Verzahnung der Serious Games mit weiteren Awareness-Materialien

Die analogen und digitalen Lernszenarien sind als alleinige Formate im Sinne der in Kapitel 2 genannten Formate, Medien bzw. Kanäle nicht ausreichend, um tatsächlich nachhaltige Security Awareness auszubilden. Bei einigen Zielgruppen existieren Widerstände gegen spielerische Formate – auch Comics sind typische Vertreter, bei denen ein glatter Riss durch die Bezugsgruppen geht, die einerseits große Fans sind und sich involvieren lassen, bei denen es andererseits jedoch ein hohes Maß an Reaktanz ausgebildet werden kann. Spiele werden dabei immer noch als Zeitvertreib und weniger als Simulation der Wirklichkeit und Entwicklungshelfer betrachtet. Bei Comics ist es oft die reduzierte Darrstellung der Figuren, denen die Betrachtenden regressive Qualitäten zuschreiben. Psychologisch ist dies aus der Perspektive dieser Gruppen nachvollziehbar, ein Nudging in Richtung wertfreier, seriöser Beschäftigung würde die Widerständler jedoch gegebenenfalls davon überzeugen können, dass diesen vermeintlich „kindlichen“ Formaten eine hohe Wirkmacht inhärent sein kann. Aus dieser Erfahrung heraus ist es also unterm Strich wichtig, den unterschiedlichen Lerntypen und zudem für diverse psychologische Verfassungen aller verschiedene Formate, Medien und Kanäle zur Verfügung zu stellen. Außerdem ist davon auszugehen, dass erstens die Serious Games ideale Beschleuniger/-innen sind, um diese im Sinne einer widerspruchsfreien Kommunikationsstrecke durch andere Formate aufzuladen (Promotion und Dokumentation) und zweitens das Durcharbeiten der Szenarien zu weiteren Bedarfen an Sensibilisierung führt, die gedeckt werden müssen, um die initiierten Sensibilisierungsaktivitäten nicht bereits von innen heraus zu kannibalisieren.

Zur Promotion vor Trainingsevents und zur Dokumentation danach eignen sich die typischen Instrumente, die im nächsten Kapitel (FAQ) beschrieben sind, etwa E-Mail (Newsletter), Intranet, Poster oder Aufsteller.

Zu den Materialien, die das Projekt „ALARM Informationssicherheit“ zur Verfügung stellt, gehören so genannte „Security Kompakt Infoblätter“, die ebenfalls aus dem Forschungsprojekt entstanden sind. Diese können als Impuls während des Awareness-Trainings eingesetzt werden [33].

Als Ergänzung und zur Diversifizierung des Game-Portfolios eigenen sich grundsätzlich alle in Kapitel 2 beschriebenen Instrumente, z. B. Artikel, Foto- und/oder Videodokumentationen.

Dabei sollte ein Intranet-Portal zum Thema Sicherheit mit unterschiedlichem Content (News, Fachartikel, Lernkarten bzw. Infografiken, Quick Guides, WBTs, FAQs, Videos, Audio-Podcasts, Minigames, Selbsttests, Moderations-Inhalte für Führungskräfte und andere Multiplikatoren etc.) stets als „Heimathafen“ einer Awareness-Kampagne betrachtet werden. Von hier aus sollten aber auch analoge Formate wie Trainings, Workshops, Events oder virale Aktionen in die Dramaturgie eingestreut werden, um echte Begegnungen mit Beziehungsmöglichkeiten und den wichtigen Face-to-face-Aspekt nicht aus den Augen zu verlieren. Außerdem ist bei digitalen Awareness-Maßnahmen über

Abb. 34 bis 39: *Digitale Serious Games 3.4.6 und bis 3.4.7 (von oben nach unten)*

Portale die Integration von Rückkanälen zum Austausch der Zielgruppen sehr wichtig, damit die Sensibilisierung nicht in reiner Lerntheorie bzw. delegierende Plattform-Awareness endet.

Wenn die analogen Serious Games „ausgespielt“ wurden, würde es sich anbieten, im nächsten Schritt Ihrer Awareness-Maßnahmen weitere gamifizierte Tools anzubieten. Dies könnten weitere Lernstationen sein, die insgesamt zu etwa 30 verschiedenen Themen angeboten werden, aber auch andere Formen wie Escape Games, Brettspiel-Events, begehbare Riesenspiele mit eingebetteten Themen-Workshops, Rollenspiele o.ä. Auf digitaler Ebene könnten thematische Selbsttests, Minigames oder serielle Verdichtungen von spielerischen Security-Aufgaben als Team-Wettbewerb innerhalb des Intranets implementiert werden.

Wenn Sie Formate nicht selber inhouse entwickeln, was vermutlich für die große Mehrheit von KMU gilt, haben Sie in Bezug auf Kauf bzw. Lizenzierung verschiedene Möglichkeiten, die Sie in Ruhe und im Vergleich sondieren und auf ihren individuellen ´bedarf hin auswählen können:

- Beratungsunternehmen der Sicherheitsbranche (Konzepte, Projektmanagement, Kampagnen i. d. R. über Partner/-innen)
- Seminaranbieter/-innen (klassisches Lernen)
- E-Learning-Anbieter/-innen (WBTs, einfache Games wie Quizze, Phishing-Tools, Videos)
- Plattform-Awareness (i. d. R. digitale E-Learning Tools, u. a. aufgeladen durch Videos, Phishing-Simulationen u. a. digitale Gadgets, bei vielen größeren Anbieter/-innen flankiert durch analoge Classroom Trainings)
- Awareness-Agenturen (mit dem notwendigen Kommunikationsfokus auf das Thema)
- Versicherungen (mit Awareness-Klausel bei gleichzeitigen Sensibilisierungsangeboten von Partnern/-innen oder Tochterunternehmungen)
- Spezialanbieter/-innen (z. B. für Gamification)

Da kostenfreie Materialien in der Regel nicht über die methodische und inhaltliche Qualität der Serious Games aus dem Projekt „ALARM Informationssicherheit“ verfügen und hier zudem synchron zur zunehmenden Wichtigkeit von Security Awareness eine hohe Marktdynamik zu erkennen ist, wurde auf konkrete Empfehlungen im Sinne von Linklisten bewusst verzichtet. Natürlich existieren diesbezüglich durchaus auch wertige Ausnahmen, die frei genutzt werden können, z. B. aus weiteren Hochschulprojekten oder einige wenige Initiativen aus dem behördlichen Umfeld. Die herausgebenden Protagonisten/-innen sind jedoch davon überzeugt, dass eine Basisrecherche nach geeigneten Ergänzungsmaterialien das von hier aus erwünschte Hineinarbeiten in das Thema ein geeignetes Kickoff-Szenario darstellt, um ein notwendiges Awareness-Konzept zu erstellen. Das mühevolle Durchkämpfen durch Elemente wie Recherche, Bewertung und Auswahl stellt mithin einen wichtigen Prozessschritt dar, geeignete Maßnahmen im Sinne der jeweils individuellen Sicherheitskultur zu finden und gegebenenfalls an die eigene Organisation anzupassen. Dieser Aspekt gilt natürlich auch für den Einkauf von kommerziellen Materialien.

3.6 Fazit

Serious Games als Bestandteil der Maßnahmen regen zum Erfahrungsaustausch an, der eine wichtige Rolle beim Erlernen neuer Inhalte darstellt. Um das ausgewählte Sensibilisierungsthema abzurunden, wird empfohlen, das thematisch passende niederschwellige Sicherheitskonzept bzw. Handlungsanweisungen mit den Teilnehmenden im Anschluss zu besprechen. Um den Erfolg von Sensibilisierungs- und Schulungsmaßnahmen zu erfassen, sollten Awareness-Messungen durchgeführt werden und Feedback zum Serious Game eingeholt werden. Dies ermöglicht Wünsche der Teilnehmenden zu berücksichtigen und sie intrinsisch zu motivieren und somit höheres Verständnis für Cyberrisiken zu erlangen. Hier können die im Projekt entwickelten Umfragen zu Informationssicherheitskultur und zur Messung des Bewusstseins für Informationssicherheit unterstützen. Es ist notwendig Sensibilisierungsmaßnahmen, wie den Einsatz von Serious Games, in regelmäßigen Abständen einzusetzen, um kontinuierliche Verbesserung des Informationssicherheitsniveaus zu erreichen. [33]

Sensibilisierung für Informationssicherheit sollte nicht als eine Einzelmaßnahme betrachtet werden. Alle Maßnahmen des vorgestellten ALARM-Gesamtszenarios können und sollten immer wieder eingesetzt werden, denn Informationssicherheit ist ein fortlaufender Prozess. Befragungen (Sicherheitskultur, Awareness-Messung) sollten wiederholt werden, analoge und digitale Serious Games können in geeigneten Situationen zur Erinnerung absolviert oder für neue Mitarbeiter/-innen als Einstieg genutzt werden. Sicherheitskonzepte, Handlungsempfehlungen, Goldene Regeln sollten präsent platziert, immer wieder diskutiert und ggf. aktualisiert werden. Damit Mitarbeiter/-innen sich leichter sicherheitskonform verhalten können, bedarf es der Unterstützung des Top-Managements des Unternehmens [37]. Durch den Einsatz von vielfältigen kreativen Methoden und gebündelten Maßnahmen entsteht durch das vorliegende Projekt ein Instrument zur Selbsthilfe für KMU, welches die Mitarbeiter/-innen befähigt, achtsamer im Umgang mit möglichen Risiken zu sein, und so zur Steigerung des Informationssicherheitsniveaus des gesamten Unternehmens beiträgt.“ [33]

Abb. 40: *Anlaloges Serious Game 3.3.7 während eines Tests durch die TH Wildau*

4 FAQ – Fragen und Antworten zur Vorbereitung, Durchführung, Moderation und Nachbereitung der

FAQ – Fragen und Antworten zur Vorbereitung, Durchführung, Moderation und Nachbereitung der analogen Serious Games

Die Inhalte des FAQ stellen einen systematisch aufbereiteten Auszug dar aus Briefings, Debriefings u. a. Settings bei als 150 Organisationen bzw. Unternehmen aus 35 Ländern. Dabei wurden Erfahrungen von Organisatoren/-innen und Moderatoren/-innen mit 40 verschiedenen Lernstationen zu Sicherheits-, Datenschutz- und Compliance-Themen berücksichtigt. Die sich aus den Fragen ableitenden Empfehlungen – insbesondere hinsichtlich Vor- und Nachbereitung, z. T. auch für die Durchführung – gelten vor allem für verzahnte Trainingsevents bei größeren KMU, bei denen z. B. synchron 4 oder mehr Stationen angeboten werden für 60 oder noch mehr Teilnehmende. Vermutlich wird sich die Beteiligung bei KKU aufgrund der Definition mit relativ wenigen Mitarbeiter/-innen in Grenzen halten, so dass die hier aufgeworfenen Fragen mit Ausnahme von Details zur Moderation für diese Unternehmen und KMU mit geringer Beteiligung wenig relevant sein dürften.

4.1 Event-Vorbereitung

Was sollte ich zuerst anbieten, die digitalen oder die analogen Serious Games?

Die Reihenfolge bleibt Ihnen überlassen. Im Sinne eines belebenden Events als Kickoff durch die analogen Szenarien und infolge der Vertiefung individueller Skills bei den digitalen wären jedoch die analogen zu priorisieren.

Wie viele Supporter werden bei einem verzahnten Trainingsevent benötigt?

Sie benötigen bei synchronem Ablauf mehrerer Stationen neben den Moderierenden – mindestens eine Person pro Station – idealerweise auch eine/n Timekeeper/-in, der/dieZeit an den Stationen überwacht, um einen reibungslosen Wechsel nach z. B. 15 Minuten zu koordinieren. Zur Moderation der komplexeren Stationen, z. B. die Spiele auf Basis von Wimmelbild-Spielfeldern, bei denen alleine die Auflösung mit dem Addieren der Punkte relativ aufwändig ist, wären zwei Moderierende ideal, da eine Moderation, die Abwechslung bietet, sich interessanter für die Teilnehmenden anfühlen dürfte und bei zwei Moderierenden pro Station gegebenenfalls auch kurzfristige Ausfälle kompensiert werden könnten. Bei größeren Trainingsevents mit mehr als 100 Personen benötigen Sie zudem eine Art Rezeptionsfunktion, die die Mitspielenden begrüßt, einweist, einteilt, gegebenenfalls auch dokumentiert und am Ende Fragebögen hinsichtlich einer Evaluation und Incentives bzw. Giveaways verteilt. Das heißt, Sie benötigen bei 4 Stationen mindestens 5 Supporter, idealerweise jedoch 10.

Welche Möglichkeiten bestehen hinsichtlich der Zahl von Teilnehmenden bei einem verzahnten Trainingsevent?

Bei maximal 12 Teilnehmenden pro Team und Station – die ideale Anzahl liegt eher bei 6-8 Personen – können Sie während eines verzahnten Trainingsevents mit z. B. 4 synchron ablaufenden Stationen und einer Stationsdauer (Bruttospielzeit) von 15 Minuten maximal 48 Personen pro Stunde per Serious Games sensibilisieren. Bei 15 – besser (hinsichtlich einer größeren Flexibilität) 30 Minuten – Pause zwischen diesen so genannten „Runs“ ist es möglich, an einem „normalen“ Arbeitstag innerhalb von achteinhalb Stunden 6 Runs durchzuführen mit einer maximalen, rechnerischen Gesamtzahl von bis 288 Personen. Bei weniger Moderierenden, z. B. 2, können diese z. B. immer noch 2 Stationen pro Kopf moderieren, so dass Sie hierbei 2 Gruppen à maximal 12 Personen pro Stunde und insgesamt dann die Hälfte der oben genannten Gesamtzahl versorgen könnten. Theoretisch ist es auch möglich, dass eine Person 4 Stationen moderiert. Allerdings würde es dann gegebenenfalls dem Moderationsprogramm an Abwechslung fehlen. Für die Teilnehmenden ist es definitiv besser und spannender, von verschiedenen Moderatoren/-innen angesprochen zu werden.

Was brauche ich zur Organisation eines verzahnten Serious Game-Trainingsevents außer dem Serious Game-Material und welchen Raum wähle ich dafür?

Neben ausreichend Tischfläche für die Spielematerialien – die Stationen mit den Wimmelbild-Spielfeldern benötigen deutlich mehr Fläche als andere – ein geeigneter Raum. Wobei Sichtbarkeit stets vor „Ruhe und Abgeschiedenheit“ gehen sollte. Das bedeutet, dass bei der Abwägung Eingangshalle eines Unternehmens versus Trainingsraum im obersten Stockwerk die Visibility für alle im Eingangsbereich höher zu bewerten ist als eine Abschottung, um gegebenenfalls Konzentration zu adressieren. Denn wir regen ja an, dass Informationssicherheit gerade über Serious Game-Trainingsevents lebendig und sichtbar gestaltet werden soll, da diese vitalisierenden Qualitäten auch auf die Awareness derjenigen einzahlen, die gegebenenfalls nicht am Trainingsevent teilnehmen, dieses jedoch bemerken und hoffentlich motiviert werden, beim nächsten Mal mit dabei zu sein. Für 4 Stationen benötigen Sie mindestens 50 qm, besser mehr. Im Zweifel verteilen Sie die Stationen auf z. B. 2 Räume. Jede moderierende Person sollte ein Smartphone als Stoppuhr verfügbar haben. Darüber hinaus sollte ausreichend Trinkwasser für die Moderierenden bereitstehen. Da das Format ähnlich einer Messesituation im Stehen stattfindet, sollten Stühle weitgehend aus dem Raum entfernt werden. Ausnahmen sind Stühle für die Moderierenden in den Pausen sowie für Teilnehmende mit körperlichem Handicap.

Können auch Mitarbeiter/-innen, die nicht aus dem Sicherheits- oder IT-Bereich stammen, Stationen moderieren?

Unbedingt, da die Inhalte der Stationen nicht explizit auf lerntheoretische Know-how-Vertiefung, sondern mit Fokus auf Diskurs, Beziehung, gemeinsames Werk, Promotion und Security als eine lebendige Story ausgerichtet sind, können auch kommunikationsstarke und motivierte Kollegen/-innen, durchaus auch Trainees oder Auszubildende, Stationen moderieren. Für den Fall von fachlichen Fragen sollte jedoch immer mindestens ein Security-Profi anwesend sein.

Wie promote ich ein Trainingsevent?

Alle Kanäle sind erlaubt. Es bieten sich in der Regel folgende an: E-Mail-Einladung (z. B. zwei Mal, etwa 5 Wochen vor dem Event und als Reminder etwa 1 Woche vorher), Intranet-Artikel (-Serie), Intranet-Banner, E-Cards, Flyer, Poster bzw. Aufsteller. Falls Sie Video- oder Audiopodcasts nutzen, sollten Sie gegebenenfalls auch darüber nachdenken, einen AV-Trailer zur Ankündigung zu produzieren. Hierbei helfen grundsätzlich Testimonials des Managements, z. B. E-Mail-Einladung signiert von der Geschäftsführung, Podcast inklusive Kurzinterview zum Format o.ä. Bei Postern bzw. Aufstellern bietet sich z. B. an, dass Sie ein generisches Motiv und Themenmotive entsprechend der Anzahl der Stationen produzieren. Die Themenmotive sollten unbedingt die verkürzten Goldenen Regeln aus den Moderationsbriefings enthalten. Sie können aber auch Themenaufsteller über eine Standauszeichnung am Tag des Events hinaus auch zur Ankündigung nutzen, indem Sie diese im Unternehmen mit zusätzlichen Terminblättern (einfach mit wiederablösbarem Kleber auf die Motive haften) platzieren.

Kann ich auch interessierte Kunden/-innen und Partner/-innen zu Trainingsevents einladen?

Ja, im Sinne von „tue Gutes und zeige es" sollten Sie durchaus auch Kunden/-innen und Partner/-innen einladen und mitmachen lassen, um zu zeigen, wie Sie Ihre Mitarbeiter/-innen sensibilisieren und um Kundenbindung zu betreiben.

Ist es problematisch, wenn bestehende Teams als Serious Game-Team auftreten bzw. wie kann ich diverse Zielgruppen mit den Serious Games ansprechen?

Die Inhalte sind grundsätzlich so gestaltet, dass verschiedene Rollen, Niveaus etc. durchaus gemeinsam angesprochen werden können. Das Einbinden von Führungskräften in Teams mit ihren Team-Mitgliedern stellt kein Problem dar, sondern kann gerade in Bezug auf die angestrebte diskursive Ebene produktiv auf Team Building-Qualitäten oder Informationssicherheit einzahlen. Die Erfahrung lehrt, dass aber vor allem diverse Teams besser im Sinn der erwünschten Diskurse funktionieren, so dass eine Durchmischung durchaus angestrebt werden sollte. Falls bestimmte Aspekte eines Themas für unterschiedliche Zielgruppen variantenreich vorbereitet werden sollen, können die Moderierenden die Moderationsinhalte so zusammenstellen, dass verschiedene Niveaus oder die Sicht unterschiedlicher Rollen gewährleistet werden kann. Die Moderationsbriefings bieten in der Regel in Bezug auf Umfang und Variation eine Grundmenge an Inhalten, die sich je nach Bedarf modular ausrichten lässt.

Wie startet ein Event und wie sollen die Teams gebildet werden?

Wenn sich spontan infolge von Selbstorganisation keine Teams abzeichnen, kann über die Rolle der bzw. des Hauptmoderierenden (Eventrezeption oder des Timekeeper/-in) eine paritätische Einteilung vorgenommen werden. Manche Organisationen arbeiten auch mit Nummernjetons von z. B. 1-4 (für die jeweiligen Teams 1-4, die vor Beginn nach einem Zufallsprinzip verteilt werden). Bei zahlreichen Ausfällen bietet es sich auch an, gegebenenfalls ein Team wegzulassen, z. B. bei 4 Stationen lediglich 3 Teams zu bilden (so dass pro Viertelstunde eine Station pausiert), denn bei weniger als z. B. 4 Teilnehmenden pro Team wirkt sich die geringere Anzahl potenziell auf die beabsichtigte Diskursqualität aus.

Warum braucht jedes Team einen Teamkapitän bzw. eine Teamkapitänin?

Der/die Kapitän/-in ist Sprecher/-in des Teams und trägt den Punktezettel bei sich. Es empfiehlt sich auch, dass sich jedes Team vor dem Start des Parcours einen sprechenden Namen gibt. Nach einer entsprechenden Ansage an alle sollte den Teams dann 60 Sekunden Zeit gegeben werden. Der Name wird auf den Punktezettel geschrieben und spontan abgefragt. Der oder die Hauptmoderierende vergibt dann optional und rein subjektiv einen Sonderpunkt für den „kreativsten" Teamnamen. Dabei sind der Phantasie keine Grenzen gesetzt.

Was bedeuten „Nettospielzeit" und "Bruttospielzeit" bzw. wie lange dauert eine Station?

Die „Nettospielzeit" umfasst die geplante Spielzeit des jeweiligen Minigame im Schritts 2 der Dramaturgie (s. Moderationsbriefings). Die „Bruttospielzeit" des gesamten Szenarios ist auf 15 Minuten hin optimiert – dies für den Fall, dass das Serious Game im Rahmen eines (gegebenenfalls incentivierten) Trainingsevents als synchronisierter Parcours mit z. B. 4 oder 6 Szenarien gleichzeitig angeboten werden. Verlängerungen als Vertiefungen in Richtung 20 oder 30 Minuten pro Station und Thema sind bei entsprechender Ausschöpfung der Inhalte der Moderationsanleitungen durchaus möglich, solange ein gleichzeitiger Wechsel der Teams an den Stationen garantiert wird. Bei Nutzung ohne Parcours-Synchronisation können sowohl Netto- als auch Bruttospielzeit frei und je nach Bedarf und z. B. Diskussionszeit bestimmt werden.

Wie werden die Punkte an den Stationen vergeben?

In jedem Game können bei Leistungserfolgen des jeweiligen Teams Punkte verdient werden. Diese Incentivierung

ist keine Pflicht, empfiehlt sich jedoch, um den sportlichen Charakter („Arena“) und die Motivation zu heben. Um die Punkte zu dokumentieren, legen Sie am besten einen Punktezettel mit einem einfachen Tabellen-Template und folgendem Inhalt an: Name des Teams, Name der Stationen, Punkte pro Station, summierte Gesamtpunktzahl. Diese Punktezettel drucken Sie auf DIN A5 oder A4 aus und verteilen je einen pro Team an den/die jeweilige/-n Teamkapitän/- (siehe nächste Antwort). Diese/-r lässt an den einzelnen Stationen die erzielten Punkte von den Moderierenden eintragen. Am Ende wird an der Event-Rezeption ausgewertet. Die Zettel bzw. Listen sind nach dem Event datenschutzsicher zu entsorgen. Für Siegerteams sollten Incentives ausgelobt werden.

Wartebereiche oder Terminvergabe – was ist besser?

Beim Einrichten von Wartebereichen ohne Voranmeldung der Teilnehmenden, startet jeweils eine Gruppe, sobald diese mit der erwünschten Anzahl an Teilnehmenden aufgefüllt ist. D. h. die Moderation an den Stationen findet nach Bedarf statt. Die Wartebereiche können dann auch dafür genutzt werden, weitere Security-Inhalte als eine Art „Amuse-Geule“ anzubieten. Ihnen sind jedoch auch etliche Nachteile inhärent. Denn mit Wartebereichen ist die Durchführung insgesamt schwerer planbar, was auch impliziert, dass es bei spontan hohem Andrang zu Staus kommen kann und Sie als Veranstalter mehr Supporter brauchen. Bei Voranmeldungen benötigen Sie mehr Zeit in der Vorbereitung, haben dann aber am Eventtag einen klaren Plan, nach dem Sie die Angemeldeten „abarbeiten“ können – es sei denn, es kommt zu kurzfristigen Absagen und unbeabsichtigten Lücken in den Teams. Bei umfangreicheren Events mit 100 oder mehr Teilnehmenden lohnt sich das Anlegen einer Exceltabelle zur Organisation der Teilnehmenden. In jedem Fall sollten Sie pro Team etwas Platz lassen für spontane Zusagen von Kolleginnen und Kollegen, die sich kurzfristig für das Event zu interessieren beginnen.

Sollte ich Serious Game-Trainingsevent verpflichtend für alle Mitarbeiter/-innen durchführen?

Eine freiwillige Teilnahme, die auch eine höhere intrinsische Motivation umfassen dürfte und per Nudge verstärkt werden kann, ist immer besser als ein Teilnahmezwang. Bei manchen Sicherheitskulturen lässt sich jedoch Druck nicht vermeiden. Bedenken Sie jedoch, dass eine verpflichtende Teilnahme bei einem Eintagesevent nicht für alle realisierbar ist (z. B. Außendienst, erkrankte Mitarbeiter/-innen, Mitarbeiter/-innen im Homeoffice) so dass mehrere Tage eingeplant werden sollten, und diese gegebenenfalls auch durch den Betriebsrat genehmigungspflichtig sein könnten. In jedem Fall (siehe auch nächste Antwort) sollte die Führungsebene als Testimonial vorangehen und eine Teilnahme mindestens als erwünscht kommunizieren.

Wie evaluiere ich den Erfolg von Serious Games?

Grundsätzlich sollten Trainingsevents von einem Fragebogen begleitet sein. Sie können darin Zustimmungen zu bestimmten Aussagen einholen, z. B. „Aufgrund der Face-to-face Kommunikation mit Moderatoren/-innen und meinem Team schätze ich den Sensibilisierungs-Wert einer Teilnahme an den Serious Games höher ein als beispielsweise ein Web Based Training, das man alleine durchführen soll“. Oder „Ich würde einem Kollegen oder einer Kollegin die Teilnahme an künftigen Serious Game-Trainingsevents empfehlen (sie/ihn dazu einladen)“. Weitere Aussagen könnten sich auf Organisation, Dauer, Strukturierung der Inhalte, Theorie-Praxis-Mix, Erwartungserfüllung, Beantwortung meiner Fragen beziehen. Zudem sollten eine Gesamtbewertung sowie Anregungen bzw. Vorschläge zur Verbesserung integriert sein.

Muss der Einsatz der analogen Serious Games mit dem Betriebsrat abgestimmt werden?

Ein Mitbestimmungsrecht des Betriebsrats bei der Durchführung von Maßnahmen der betrieblichen Weiterbildung nach § 98 Abs. 1 BetrVG erstreckt sich auf jede Form einer Wissensvermittlung. Da es bei den Serious Games nur sekundär um klassische Weiterbildung geht, liegt unserer Auffassung nach kein abstimmungspflichtiges Format vor. Um potenzielle Konflikte zu vermeiden, sollte eine Mitbestimmung des Betriebsrats in Einzelfällen abgeklärt werden. Da zudem das Punktesystem an den Stationen ausschließlich hinsichtlich der Incentivierung vorgesehen ist und keine Datenverarbeitung über die Leistung bzw. Verhalten der Arbeitnehmenden nach § 87 Abs. 1 Nr. 6 BetrVG vorgesehen ist, müssen, unserer Auffassung nach, auch die Team-Bewertungen nicht mit dem Betriebsrat abgestimmt werden.

Sollten Zertifikate über die Teilnahme ausgegeben werden?

Falls die Serious Games als betriebliche Weiterbildung gewertet werden und z. B. andere Formate wie verpflichtende E-Learnings ersetzen, sollte über die Ausgabe von Teilnahme-Zertifikaten nachgedacht werden. Die Bedeutung derartiger Zertifikate hängt in der Regel vom Wert ab, dem man diesen innerhalb der Unternehmenskultur beimisst. Im Fall einer Zertifikatsausstellung sollte jedoch die potenzielle Zustimmungspflicht eines Betriebsrats geprüft werden.

Welche Werbemittel eignen sich grundsätzlich als Giveaway oder Incentive für das Thema Informationssicherheit?

Zum Beispiel

- Tools mit originären Security-Funktionen, z. B. Klassifikationsdrehscheibe und andere Funktionskarten
- Objekte zur paradoxen Intervention, z. B. „Passworthalter“ mit Passworthalterkarte, „VirusBrickMaster“-Baustein-Box zur Imagination von Malware
- Streuartikel mit security-affinen Botschaften, z. B.

Stressbälle – und -figuren, aufblasbare Nackenkissen, Schirme, Tassen, Trinkflaschen, Tablettaufleger, Stifte, Tile Tracker, (Haft)Notizblöcke, Stifte, T-Shirts, Pflasterhefte, Lanyards u. v. m.

- Security-affine Streuartikel für die praktische Anwendung, z. B. Kryptonizer, Webcamcover, USB Sync Stopper, Anti-Skimming-Cards bzw. -Etuis u. v. m.
- Awareness-Jahreskalender als Security-Memorizer
- Security Card Games
- Security-Koffer zur Anwendung diverser Tools für Führungskräfte [36]

Welche Werbemittel sind geeignet, um ein Trainingsevent als Giveaways bzw. Incentives aufzuladen?

Falls Sie Punkte vergeben, sollten die Gewinner-Teams ein Incentive erhalten. Es bleibt Ihnen überlassen, ob Sie alle Rundensieger (Gewinner-Team pro „Run“) oder bei mehreren „Runs“ lediglich eine/-n Tagessieger/-in auszeichnen bzw. ob Zweit- und Drittplatzierte ebenfalls einen Preis erhalten (manche Organisationen loben auch Preise für saisonale Siegerteams aus, wenn sie das Format als Roadshow durch mehrere Standorte schicken). Nutzer dieses Formats loben als Incentive wertige Streuartikel – oft mit Security-Bezug – z. B. mit Security-Botschaften bedruckte Schirme oder T-Shirts- aus. Populär sind auch Gutscheine, z. B. für Team-Events mit Sicherheitsbezug (Rafting, Fallschirmspringen etc.). Bei den Giveaways, die – anders als die Incentives – nur die Sieger-Teams erhalten, alle Teilnehmenden des Events als eine positiv aufgeladene Erinnerung mitnehmen sollten, sind insbesondere Streuartikel mit Security-Bezug oder bedruckte Tassen o.ä. sehr beliebt. Nicht zu unterschätzen ist ein Trainingsevent auch als eine Plattform zum Verteilen von Quick Guides oder anderen Printartikeln mit Security-Bezug, z. B. eine Informationsklassifikations-Drehscheibe. Gerade die Synergieeffekte zwischen live diskutierten Regeln, Tipps und Tricks und in Quick Guides gedruckten sind ideal nutzbar, um die Penetration einer Regel-Promotion zu erhöhen, denn ein Quick Guide oder ein anderes Printprodukt zum Thema, das aus einem als positiv wahrgenommenen Event mitgenommen wird, strahlt potenziell eine ganz andere, erhöhte Wirkung aus als eine security-affine Anlage einer E-Mail oder einer Gehaltsabrechnung.

Darf auf Trainingsevents fotografiert werden?

Aus Datenschutzgründen müssen alle Teilnehmenden ihre Zustimmung geben. Es empfiehlt sich allerdings alleine aus Gründen einer kommunikativen Nachbetrachtungsstrecke, ein Event unbedingt per Videos und/oder Fotos zu dokumentieren. Idealerweise auch nicht vergessen Team-Fotos zu erstellen, vor allem von dem bzw. den Siegerteam(s) – am besten gleich mit dem Team-Preis.

Was muss ich im Kontext der Nutzungsrechte beachten?

Die Nutzungsrechte der hiesigen analogen Serious Games umfassen für alle Nutzenden eine Anwendung im Rahmen der jeweils internen Kommunikation der Bezugspersonen. Die kommerzielle Nutzung, d. h. eine kostenpflichtige Durchführung bei Kunden/-innen der jeweiligen Anwendenden, eine kostenpflichtige, Vermietung bzw. ein Verkauf o.ä. ist – auch bei Änderung des Contents – untersagt.

Wo finde ich weitere Informationen?

Detaillierte Regelwerke, Content zum jeweiligen Thema sowie Spiel- und Moderationsanleitungen präsentieren die zu den Serious Games gehörenden Moderationsblätter. Die Materialen, Spielmaterial, Moderationsblätter und Anleitungen zum Ausdrucken und Finalisieren hinsichtlich der konkreten Nutzung, sind über die Projektwebseite https://alarm.wildau.biz/ downloadbar. Ein fertig konfektionierter Spielekoffer mit allen 7 Serious Games zum sofortigen „Losspielen“ („out of the box“) ist beim Projektpartner known_sense (sense@known-sense.de) kostenpflichtig bestellbar.

Ich habe eine generelle Frage zu den Serious Games oder zu den Inhalten der Serious Games bzw. der Moderationsbriefings, die nicht über die Projektdokumente beantwortet werden kann. Wie bekomme ich die passende Antwort dazu?

Da das Projekt „ALARM Informationssicherheit“ abgeschlossen ist, können Sie sich in Bezug auf methodische Fragen, bei Nach- oder Ergänzungsbestellung an den Projektpartner known_sense (sense@known-syense.de) wenden. Beratungsleistungen sind kostenpflichtig. Bei inhaltlichen Fragen zu Details im Kontext Informationssicherheit empfehlen wir eine entsprechende Online-Recherche.

4.2 Event-Durchführung

Wie reagiere ich, wenn Moderierende oder andere Rollen kurzfristig ausfallen?

Wenn Sie idealerweise jede Rolle doppelt besetzt haben, sollte das Trainingsevent dennoch durchführbar sein. Ansonsten finden Sie vielleicht kurzfristig Kollegen/-innen, die Sie unterstützen.

Welche Werbemittel bieten sich an, um die Sichtbarkeit des Trainingsevents zu erhöhen?

Z. B. generische Werbeaufsteller oder Bildschirme bzw. Beamer-Präsentationen mit Key Visual im Eingangsbereich, Themenaufsteller, -poster und/oder -Lernkarten an den einzelnen Stationen, Präsentationen von Incentives bzw. Giveaways im Eingangsbereich – bei KKU-Veranstaltungen vermutlich nicht notwendig.

Worauf sollte ich bei einem Trainingsevent außerdem achten?

Ausreichend Getränke für Moderation und Teilnehmende zur Verfügung stellen und eine motivierende und den Ablauf kurz erklärende, ein bis zweiminütige Einführung für alle Teams jedes „Runs“ einplanen

4.3 Moderation

Wofür bin ich als Moderator/-in beim Trainingsevent grundsätzlich zuständig?

Im Rahmen einer Train-the-trainer-Session lernen, wie man moderiert (dies kann auch per Videokonferenz erfolgen), aus dem Pool an Goldenen Regeln und Fragen 2-3 aussuchen, die in die Team-Diskussionen eingebaut werden sollen, am Tag selbst die Stationen einrichten und das Spielematerial managen, an der Station die Teams begrüßen und in das jeweilige Thema einführen, circa 15 Minuten pro Team moderieren, jeweils das Spiel in Schritt 2 erklären und bei Incentivierung kommunizieren, wie viele Punkte man gewinnen kann, jede Runde mit Lösung im Sinne eines Debriefings abschließen und bei Incentivierung Punktezahl jedes Team auf der Punktekarte dokumentieren.

Wie gehe ich bei der Moderation der Serious Games vor?

Grundsätzlich bleibt es Ihnen überlassen, wie Sie eine Station moderieren, sofern der abgesprochene Zeitrahmen bei Vernetzung mit anderen Stationen eingehalten wird. D. h. der Ablauf in den Moderationsbriefings ist als Vorschlag zu betrachten. Wenn Sie sich z. B. damit wohler fühlen, mit dem Spiel zu starten (Schritt 2), wäre dies durchaus in Ordnung, wenn der Diskurs insgesamt nicht zu kurz kommt. Wichtig ist also, dass Sie die Teilnehmenden in das Thema involvieren. Die ideale Moderation referiert nicht ausschließlich, sondern lässt dem Team Räume für Diskussionen.

Darf ich Moderationsbriefings bzw. Lösungsblätter auf meine Station mitnehmen?

Ja, als Gedächtnisstütze, um z. B. in den Moderationspausen nachzuschauen. Sie sollten jedoch in der Face-to-face-Situation nicht vom Blatt ablesen.

Wie viele Fragen bzw. Goldene Regeln bespreche ich pro Session?

Um lebendige Diskurse zu initiieren, reichen oft ein oder zwei grundlegende Ausgangsfragen, die die Teilnehmenden entsprechend berühren. Diese ergeben sich aus dem Thema bzw. aus den Vorschlägen für Fragen in den Moderationsbriefings. Dabei müssen weder alle hier gelisteten Fragen, noch alle Goldenen Regeln im Sinne einer Vollständigkeit oder Reihenfolge abgearbeitet werden. Wählen Sie am besten im Rahmen Ihrer Vorbereitung 2-3 Fragen und Goldene Regeln aus, die Sie persönlich wichtig finden oder leichter als andere moderieren können. Streuen Sie diese dann anlassbezogen in Ihre Moderation ein, d. h. Sie sollten am besten Diskussionspunkte des Teams aufgreifen, um Ihre vorbereiteten Inhalte passend zu integrieren. Denken Sie immer daran: Es ist „Ihre“ Moderation, bei der kaum „richtige“ oder „falsche“ Pfade entstehen, solange das Thema im intendierten Sinne behandelt wird.

Muss ich stets sämtliche zusätzliche Fragen eines Absatzes stellen, die den Hauptfragen folgen?

Nein. Fragenkaskaden dienen in der Regel dazu, von allgemeinen Antworten zu vertiefenden zu führen oder aber, um verschiedene Aspekte eines Themas anzusprechen. Ihre Anordnung im Rahmen eines Fragenblocks fordert nicht ausschließlich eine der Reihenfolge entsprechende Dramaturgie. Fragen Sie idealerweise nach den Aspekten, die Ihnen am wichtigsten erscheinen und wählen Sie entsprechende Fragen aus, während Sie andere vernachlässigen können, wenn sie Ihnen weniger wichtig erscheinen.

Was tun, wenn während der Moderation Fragen aufkommen, die ich nicht beantworten kann?

Reagieren Sie möglichst entspannt und authentisch, da es bei der Behandlung der Inhalte nicht um einen Wissenswettbewerb geht. Unter Umständen können Sie eine Klärung bis zum nächsten Meeting in Aussicht stellen oder aber Sie beteiligen bei der Suche nach einer Antwort auch das Team bzw. einzelne Teammitglieder. Hierbei sollte deutlich werden, dass Sicherheit bzw. Datenschutz und die Klärung einzelner Sicherheitsfragen tatsächlich auch Teamwork bedeuten.

Wozu dienen die so genannten „projektiven Fragen“? Welche Ziele kann ich damit erreichen? Wo liegen die Grenzen?

Über projektive Fragen wollen wir bewirken, dass sich die Teilnehmenden u. a. mithilfe von Metaphern bzw. Imaginationen in eine andere Person oder in eine von der Wirklichkeit abweichende Logik (Psycho-Logik) hineinversetzen (z. B. „Sicherheit als Farbe“). Sie eignen sich vor allem dann, wenn die Mitarbeiter/-innen sich z. B. vor der direkten Bewertung einer Situation scheuen. Psychologisch nutzt eine projektive Fragestellung die Erfahrung, dass es uns allen offenbar leichter fällt, über andere und deren Verhaltensweisen zu sprechen als über unsere eigenen. Erfahrungsgemäß fällt es manchen Personen schwer, ihre Realität hinter sich zu lassen, so dass bei Widerständen bestimmter Personen gegenüber projektiven Fragen „Brücken“ gebaut werden sollten, um diesen den Zugang zu Projektion zu erleichtern. Sie können dies unterstützen, indem Sie sich auf projektive Fragen vorbereiten und während der Beantwortung auch persönliche Assoziationen integrieren.

Könnte es passieren, dass Teilnehmende auf einzelne Fragen nicht oder aggressiv reagieren, weil sie diese überfordern oder Ihnen zu persönlich vorkommen? Wie gehe ich damit um?

Die Komplexität von Sicherheit und Datenschutz wird nur dann sichtbar, wenn wir auch über den persönlichen Umgang mit diesem Thema sprechen. Manche Teilnehmende werden sich potenziell eher zurückhaltend zeigen. Wenn jedoch andere, darunter auch Sie in Ihrer Moderation, offen und möglichst authentisch über die einzelnen Themen sprechen, besteht die Chance, dass sich auch die „Stillen“

daran beteiligen. Sollte spürbar sein, dass jemand mit einer Diskussion oder Aufgabe überfordert ist, akzeptieren Sie die vermutlich daraus resultierende Zurückhaltung. Wenn diese Zurückhaltung allerdings zum Dauerbrenner wird oder sich in Richtung Aggression entwickelt, suchen Sie u. U. ein Vier-Augen-Gespräch mit der entsprechenden Person und erkundigen Sie sich nach den Gründen.

Wie reagiere ich, wenn Team-Mitglieder im Laufe von Diskussionen potenziell (eigene) Verstöße schildern?

Verhindern Sie, dass Teilnehmende an den Pranger gestellt werden. Sollte ein Verstoß offensichtlich werden, sprechen Sie die Person, die über den Verstoß gesprochen hat, unter vier Augen an und entscheiden Sie im Einzelfall über Konsequenzen.

Wie verhalte ich mich, wenn Teilnehmende versuchen, mir die Moderationsrolle bzw. Lead zu nehmen?

Solange ich in der Lage bin, die Kommunikation wie gewünscht zu steuern, ist es zweitrangig, wer innerhalb des Teams die verbale Führungsrolle übernimmt.

Wie reagiere ich, wenn jemand aus dem Team bei Diskussionen um z. B. offene Fragen aus dem Moderationsbriefing potenziell „falsch" antwortet?

„Falsch" (im Sinne eines nicht abgedruckten Wortlautes) ist bei offenen Fragen sogar ausdrücklich erwünscht, zeigt dies doch, dass die zugehörige Frage offensichtlich ihre Berechtigung hat. Möglicherweise ist die Frage aber auch missverständlich formuliert oder das Umfeld, auf das sich Frage und Antwort beziehen, hat sich mittlerweile geändert. Dies wäre ein guter Grund, Inhalte oder Formulierung anzupassen. Keinesfalls sollte einem Teammitglied das Gefühl vermittelt werden, dass es bei der Besprechung der Karten um einen Leistungstest o.ä. geht.

Wie reagiere ich, wenn sich komplette Teams oder einzelne Teilnehmende nicht aktiv oder nicht ausreichend an Diskussionen bzw. den Spielen beteiligen?

Sprechen Sie nach Möglichkeit selbst mit großen persönlichen Anteilen über das von Ihnen moderierte Thema und motivieren Sie ein eher passives Team durch zugespitzte Fragen im Kontext des Themas. Widerständige Situationen einzelner lösen sich in der Regel nach wenigen Minuten von selbst auf, da die Widerständigen relativ schnell bemerken, dass ein strategischer Widerstand deutlich anstrengender ist als das Mitspielen bzw. als eine soziale Integration ins Team.

Wie reagiere ich in meiner Moderation, wenn Teilnehmende das Format nutzen, um Unzufriedenheit mit dem Security Management, der IT, unserer Führung oder generell dem Unternehmen auszudrücken?

Sollte Unzufriedenheit nachvollziehbar argumentiert werden und einen Kontext zu den Inhalten der Station aufweisen, thematisieren Sie dies innerhalb des Teams. Dokumentieren Sie die Argumente und sprechen Sie darüber mit den zuständigen Personen, die in der Sache unterstützen könnten. Bei fachfremder Kritik sollte es Ihnen überlassen sein, ob Sie potenzielle Kritik gegebenenfalls an die entsprechenden Stellen weitertragen. Das Desavouieren einzelner Personen hat in einem derartigen Setting keinen Platz. Fordern Sie entsprechende Personen auf, dieses zu unterlassen.

Wie kann ich bestimmte Situationen, z. B. wenn Team-Mitglieder Fragen nicht verstehen oder offensichtlich Probleme haben, bestimmte Fragen zu beantworten, lebendiger gestalten?

Idealerweise sind Sie so gut vorbereitet, dass Sie in zähen Momenten über Ihre persönlichen Anliegen und Erfahrungen im Kontext des Themas sprechen können und das Team so motivieren, Ihre Statements zu kommentieren. Wenn Sie darüber hinaus aber in der Lage sind, Schweigen bzw. Passivität auszuhalten, können Sie sich auch überlegen, warum das Team

bei bestimmten Themen nicht mitzieht und gegebenenfalls damit verbundene Tabus ansprechen, denn der Grad der Gruppenaktivität wird einen direkten Bezug zu den Inhalten aufweisen.

Wie reagiere ich, wenn mir innerhalb der Moderation auffällt, dass sich die Diskussion zu weit von der Ausgangsfrage entfernt?

Sie haben verschiedene Möglichkeiten der Intervention. Leiten Sie die Diskussion zurück zum Ursprungsthema, brechen Sie die aktuelle Diskussion zugunsten der geplanten ab oder nehmen Sie diesen „Umweg" hin, weil er für Sie und/oder das Team potenziell nützlich sein könnte.

Wie reagiere ich, wenn die Mitspielenden jedes singuläre Spielszenario ausgiebig diskutieren oder aus anderen Gründen so langsam agieren, dass die vorgesehene Spielzeit potenziell nicht ausreichen würde.

Sie müssen in Ihrer Moderation auf Basis der Stoppuhrfunktion Ihres Smartphones mit regelmäßigen Durchsagen der noch vorhandenen Zeitreserven reinen produktiven Zeitdruck entwickeln, denn in der Arbeitswirklichkeit erledigen die Kollegen/-innen ja ihre Arbeit in der Regel auch unter Zeitdruck, so dass die Serious Games auch über den Faktor Zeit die Wirklichkeit abbilden. Bei Spielkarten kann nicht jeder Detailinhalt von allen im Team gelesen, behandelt und diskutiert werden. Lassen Sie daher, wenn dies nicht bereits in Selbstorganisation passiert, Kleingruppen innerhalb des Teams bilden, die synchron an der Lösung arbeiten. Falls dann am Ende noch Spielzeit übrig sein sollte, lassen Sie das Team als Ganzes das Big Picture der Lösung beurteilen und gegebenenfalls korrigieren. Das heißt, nicht jede/-r beschäftigt sich mit allen Inhalten – dies ist auch nicht notwendig, da es ja primär bei den Serious Games nicht um eine reine Wissensvermittlung geht.

Wie reagiere ich, wenn die empfohlene Bruttospielzeit von 15 Minuten bei synchronen Trainingsevents abgelaufen ist und das Team an meiner Station noch diskutiert?

Die Diskussion muss bei verzahnten Stationen eines Parcours abgebrochen werden, da der synchrone Wechsel essentiell für das Gelingen dieses Formats ist. Sie können den Teilnehmenden jedoch anbieten, nach Ablauf des „Runs", also nach dem Durchlaufen aller Stationen" bei entsprechenden Pausenzeiten vor Beginn eines nächsten „Runs" weiter zu diskutieren.

Darf ich die Inhalte der Moderationsbriefings hinsichtlich der internen Anwendung ändern?

Ja, Sie müssen vor allem bei sehr generischen Zusammenhängen entsprechende Individualisierungen im Sinne der Sicherheitskultur und Policies in Ihrem Unternehmen anpassen und sich gegebenenfalls auch Notizen dazu machen.

Wer hilft mir dabei, meine Moderations-Kompetenz zu verbessern, wenn ich bemerke, dass ich persönlich unsicher bin oder meine Fähigkeiten nicht ausreichen, die Inhalte adäquat zu vermitteln?

Bei fachlichen Vakanzen: Sprechen Sie mit der IT bzw. dem zuständigen Sicherheitsmanagement und fragen Sie nach Hilfsmitteln, Links, Trainings. Bei Aspekten der Moderation fragen Sie ebenfalls moderierende Kollegen/-innen nach Tipps oder organisieren Sie sich passende Fachliteratur bzw. Seminare.

4.4 Event-Nachbereitung

Welche Kommunikation empfiehlt sich im Zuge einer Dokumentation?

Im Sinne einer widerspruchsfreien Kommunikationsstrekke von der Promotion über den Event bis hin zur Nachbetrachtung empfiehlt es sich, mindestens einen Artikel über interne Kanäle wie Intranet oder Mitarbeitendenmagazin (gegebenenfalls auch in einem Kundenmagazin oder –Newsletter) zu platzieren. Aufhänger könnten eine Darstellung der Siegerteams inklusive Fotos und O-Töne von Teilnehmenden (siehe Fragebogen), aber auch die Auswertung des Fragebogens selbst sein mit einem Ausblick auf kommende Awareness-Aktivitäten, da über ein Trainingsevent bekanntermaßen Bedarfe nach weiterer Sensibilisierung erzeugt werden.

Wie werte ich die optionalen Fragebögen der Teilnehmenden aus?

Über einen Fragebogen können Sie evaluieren, wie die Teilnehmenden das Format bewerten, nicht jedoch die Wirkung der Maßnahme selbst. Hierfür benötigen Sie weitere Werkzeuge, die im Kapitel über Evaluationen benannt sind.

In welchen Zyklen biete ich Serious Game-Events an?

Es spricht methodisch nichts dagegen, jede/n Mitarbeiter/-innen einmal pro Jahr durch einen Lernparcours zu schikken. Bei Verzahnung von z. B. 4 Stationen zu einem Trainingsevent blieben für das 2. Jahr noch 3 Stationen aus dem ALARM-Gesamtportfolio – es sei denn, Sie kaufen noch eine weitere Station dazu und hätten dann nochmals 4. Sie können natürlich auch punktuelle Deep Dives mit einzelnen Stationen bzw. Themen anbieten oder beides miteinander kombinieren.

Was unternehme ich, wenn alle oder die meisten Mitarbeiter/-innen alle Serious Games absolviert haben?

Sie können weitere Serious Games dazu kaufen oder in andere Maßnahmen überführen. In Bezug auf Gamification existieren zahlreiche weitere Ansätze von kurz bis lang, analog oder digital, die Sie nutzen können.

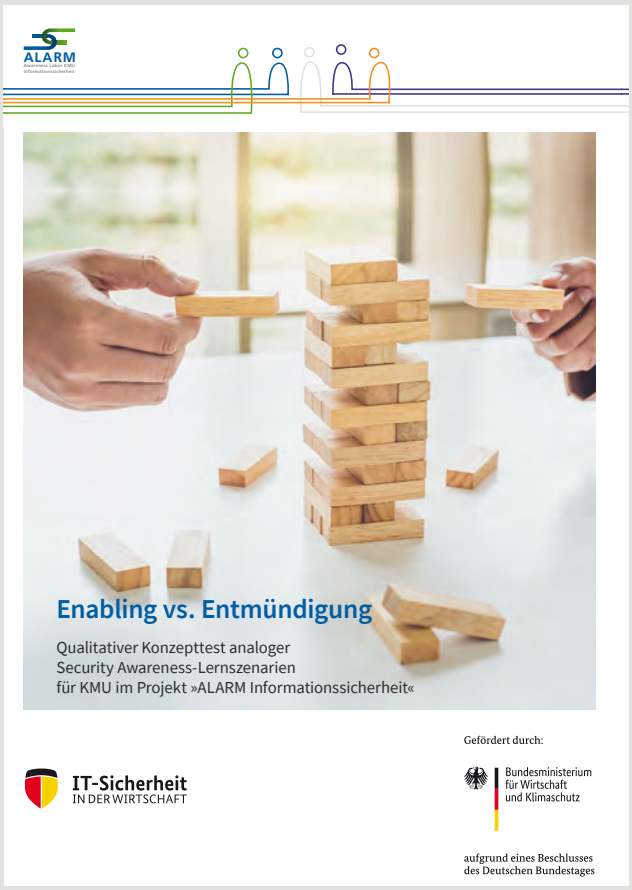


Abb. 41 und 42: *Cover der beiden Vorgängerstudien [11] und* [29]

5 Erkenntnisse aus dem Gesamtszenario und den drei Studien des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“

5.1 Zusammenfassung im Kontext weiterer wissenschaftlicher Literatur

Es besteht kein Zweifel, dass Cyberattacken existenzbedrohlich für kleine und mittlere Unternehmen (KMU) werden können und die Rolle der Informationssicherheit im deutschen Mittelstand immer wichtiger wird [38]. Unternehmen müssen weltweit dem Informationssicherheitsmanagement (ISM) zunehmend Priorität einräumen [39]. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) macht immer wieder und aktuell klar, dass deutsche KMU die Lage ihrer eigenen IT-Sicherheit im Fokus ihrer Geschäftsprozesse haben müssen [40]. Laut der Studie des Dachverbands der Industrie und Handelskammern (DIHK) für Deutschland haben die Cyberangriffe des vergangenen Jahres gezeigt, dass jedes Unternehmen zum Ziel von Hackerinnen und Hackern werden kann [41]. KMU sind somit keineswegs ausgenommen. Allerdings hielten die Wirkung bisheriger Maßnahmen zur Erhöhung des Informationssicherheitsbewusstseins und ein sicherheitsrelevantes Verhalten von Mitarbeitenden nicht an [42] [43]. Deutsche Unternehmen haben dabei die Gefahren vielfältiger Cyberangriffe durchaus erkannt, treffen aber lediglich überwiegend technische Vorkehrungen [41]. Diese sind ohne Frage eine wichtige Komponente der Informationssicherheit, aber gegen anwachsende Cyber- und Realangriffe wie Social Engineering allein kein adäquates Mittel [44]. Demgegenüber gab es keinen nennenswerten Anstieg an organisatorischen Maßnahmen für Informationssicherheit und nur ein Drittel der in der DIHK-Studie befragten Unternehmen verfügt über einen Notfallplan [41]. Dieser Widerspruch zeigt ein Paradoxon, das in deutschen Unternehmen existiert, mit einem offensichtlichen Mangel an nachhaltiger Umsetzung von Sensibilisierungsmaßnahmen zur Informationssicherheit, insbesondere in KMU.

Keine Steigerung der organisatorischen Maßnahmen für Informationssicherheit in deutschen KMU bedeutet keine Awareness-Förderung und keine Sensibilisierungsmaßnahmen für Führungskräfte und Mitarbeitende. Damit sind die Mitarbeitenden der deutschen KMU nicht ausreichend sensibilisiert und geschult, obwohl dies von den BSI-Standards [45] und der internationalen Normfamilie ISO/IEC 2700X [46] explizit gefordert wird. Ein betriebliches Informationssicherheitsmanagementsystem (ISMS) ist ohne solche Sensibilisierungs- und Schulungsmaßnahmen eindeutig unvollständig [47]. Zudem ist die wirtschaftliche Verflechtung erheblich und auch international gibt es deutliche Indizien dafür, dass unsicheres Verhalten von Mitarbeiterinnen und Mitarbeitern eine große Bedrohung darstellen und die Cybersicherheit in Unternehmen untergraben kann [48]. Um Cyberbedrohungen wirksam entgegenzuwirken, sind Programme zur Sensibilisierung für Informationssicherheit (Information Security Awareness (ISA)) ein wesentlicher und unstrittiger Eckpfeiler der Unternehmenssicherheit, wobei es viele Möglichkeiten gibt, Wissen über Informationssicherheit zu vermitteln. Aber Wissen allein genügt nicht. Die Forschungsergebnisse vieler internationaler Studien sind zu beachten, wonach eine reine Wissensvermittlung keineswegs ausreicht um ein nachhaltiges Informationssicherheitsbewusstsein zu erreichen [24]. In dem vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) von 2020 bis 2023 geförderten Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ wird daher ein Gesamtszenario für neue Wege zu mehr nachhaltiger Informationssicherheit im deutschen Mittelstand entwickelt, das den Menschen in den Mittelpunkt stellt. Neben umfangreichen Literaturrecherchen zur Situation in Unternehmen wurde im Projekt der aktuelle Stand der Informationssicherheit und des Informationssicherheitsbewusstseins (ISA) durch eine Kombination verschiedener Methoden erfasst [38], [49].

Die hier vorliegende dritte Studie des Projekts „ALARM Informationssicherheit“ rundet den Reigen der Projektstudien durch ein „Desk Research“ des Unterauftragnehmers known_sense ab. In der ersten Studie [11] [50] wurden von known_sense tiefenpsychologische Interviews mit den beteiligten Pilotunternehmen durchgeführt, um beispielhaft den Ist-Stand der Informationssicherheit in KMU zu erfassen und daraus die relevanten Themen für die Entwicklung von adäquaten analogen Sensibilisierungsmaterialien zu identifizieren. Diese Erkenntnisse, gepaart mit einer Online-Umfrage (Report 1 [51]), bildeten auch die Grundlage für die Entwicklung der im Gesamtszenario integrativ verzahnten digitalen Lernszenarien und „Vor-Ort-Angriffe“. Das Ziel des Projektes war von Beginn an, dass von der betrieblichen Alltagssituation ausgegangen werden sollte, um eine wissenschaftlich fundierte und gleichzeitig ganz praktische Hilfe für KMU zu entwickeln. KMU sollen die eigene Etablierung von Sensibilisierungsmaßnahmen für die Mitarbeitenden vorantreiben können und so zur Erhöhung der betrieblichen Informationssicherheit und zum Aufbau einer angemessenen KMU-Sicherheitskultur beitragen und letztlich die Erhöhung des Sicherheitsniveaus in deutschen KMU absichern.

Der Faktor Mensch spielt in der Informationssicherheit eine immer bedeutender werdende Rolle. Das Benutzerverhalten gilt inzwischen weithin als entscheidender Bestandteil der Cybersicherheit und Schulungen sind die am häufigsten empfohlene Methode zur Gewährleistung von sicheren Verhaltensweisen [52], wobei meistens keine Aussagen zu den Methoden und zur Didaktik erfolgen. Aber solche

Aussagen wären durchaus von Bedeutung. Da einerseits das digitale Zeitalter die Interaktion mit digitalen Diensten (Online-Services) erfordert, wird ISA aller Menschen wichtiger denn je. Da andererseits ISA inzwischen als eine Reihe von Aspekten definiert ist, reicht es nicht aus, einfach nur das Wissen zu erweitern [53]. Das macht die Effizienzsicherung von Sensibilisierungs- und Schulungsmaßnahmen für Informationssicherheit äußerst diffizil. Gerade angesichts der bedeutenden Rolle, die Einzelpersonen für das Wohlergehen der Sicherheit von Organisationen spielen, werden die Endbenutzenden von IT-Systemen dazu ermutigt, sich selbst als Teil der Informationssicherheitslösung zu sehen, und es wird von ihnen erwartet, dass sie bestimmte Sicherheitsfunktionen übernehmen (z. B. nach dem Motto „Backend-Human-Firewall"). Allerdings besteht häufig eine Kluft zwischen den Erwartungen der Institution an die Informationssicherheitsrolle der Endbenutzenden und deren funktionale Rolle [54]. Aus Wissen folgt nicht einfach linear auch ein tatsächlich sicherheitsrelevantes Verhalten.

Es wurde durch die intensive Befragung der Pilot-KMU deutlich [11] [50], dass es sich nicht um neue Bedrohungen, sondern um alt bekannte Sicherheitsprobleme handelt, mit denen sich die deutschen KMU noch immer auseinandersetzen. Zudem verdeutlichen die von den Interviewten genannten relevanten Themen, dass der Awareness-Reifegrad oft deutlich ausgebaut werden kann, denn auf den ersten beiden Plätzen liegen die altbekannten Problemfelder Passwortsicherheit und Phishing-Attacken [11] [50]. Die insgesamt acht erkannten Problemkomplexe der KMU wurden zu sieben Themen verschmolzen, die die Grundlage der Entwicklung von jeweils sieben analogen und digitalen, gamifizierten Lernszenarien (Serious Games) und „Vor-Ort-Angriffen" darstellten. Gerade die umfassende Digitalisierung der Geschäftsprozesse erfordert dabei durchaus eine analoge Sensibilisierung. Merkmale unserer modernen spielebasierten analogen Sensibilisierung mit Nachhaltigkeit zur Informationssicherheit und Datenschutz sind:

- Aktive Partizipation der Teilnehmenden
- Begreifbar machen durch Haptik
- Begreifbar machen durch interaktives Tun
- Begreifbar machen in einem diskursiven Setting
- Erinnerung durch Geschichten/Erzählungen beflügeln
- Eigene Erfahrungen einbringen können
- Zeitlich flexible Gestaltung (von 15 Minuten in der Pause bis eine Stunde für Intensivierung).

Wissenschaftlich anerkannt ist seit Jahrzehnten, dass vor allem ein Mix aus verschiedenen Methoden für die unterschiedlichen Zielgruppen, verschiedenen Lerntypen und abstrakten Themen notwendig ist [55]. Unser Projekt hat daher neben den analogen Serious Games auch auf die Entwicklung von ergänzenden digitalen Serious Games [49] [56] [57] gesetzt, die über die Projektwebseite [7] zum individuellen Spielen aufgerufen werden können. Wichtig ist bei der betrieblichen Nutzung der digitalen Serious Games, dass eine Nachbesprechung im Team erfolgt, um den diskursiven Charakter zu stützen. Darüber hinaus wurden passende „Vor-Ort-Angriffe" (Simulationen, Vor-Ort-Begehungen) durchgeführt, deren Erkenntnisse sich in Handlungsanweisungen und niederschwelligen Sicherheitskonzepten für KMU widerspiegeln [7] [49]. Zudem sind unsere behandelten Themen zur Sensibilisierung für Mitarbeitende nachhaltig interessant, da alle Themen auch für das Privatleben wichtig und nutzbar sind – ein Aspekt, dessen Bedeutung in der empirischen Literatur (z. B. [58]) und in der wissenschaftlichen Literatur (z. B. [59] [60]) immer wieder hervorgehoben wird.

Die Erkenntnis aus den Befragungen der Studie 1 [11] war, dass Gamification mit spielerischen und erlebnisorientierten Lernszenarien die Mitarbeitenden deutlich anspricht und deren Phantasie zum abstrakten Thema belebt, gleichzeitig aber nicht ohne strategische Vorbereitung und regelmäßige inhaltliche Begleitung erfolgen darf. D. h., humorvolle Maßnahmen in deutschen KMU müssen mit strategischer, respektvoller Ansprache flankiert werden und das Spielerische darf nicht zu sehr in den Vordergrund treten, um die Akzeptanz nicht zu gefährden [11]. Darüber hinaus bedarf es eines klaren Planes für die zum Thema passenden Narrative sowie ansprechende Formulierungen in einer für KMU passenden Art und Weise und eines aktiven Austausches. An dieser Stelle wird bereits eine weitere Empfehlung für die Implementierung in deutschen KMU deutlich: Die Etablierung der Rolle und Funktion einer Moderatorin/eines Moderators innerhalb des KMUs als strategisches Element des Aufbaus der Sicherheitskultur und als praktische Umsetzungshilfe für eine kontinuierlich durchzuführende Sensibilisierung zu aktuellen Themen. Ob dies mit anderen Rollen/Funktionen wie die einer/eines Informationssicherheitsbeauftragten [47] kombiniert werden kann, ist im Top-Management des KMU zu entscheiden.

Sowohl die BSI-Standards [45] und ISO/IEC-Normfamilie 2700X [46] als auch die wissenschaftliche Literatur gehen von zielgruppenorientierten Sensibilisierungs- und Schulungsmaßnahmen für die Mitarbeitenden aus. Zudem ging bereits die konzeptionelle Idee des Projekts „ALARM Informationssicherheit" im Projektantrag davon aus, dass die Themen für mehr Informationssicherheit in KMU spezifiziert nach den betrieblichen Tätigkeitsprofilen erfolgen sollten. Die erste Studie [11] brachte demgegenüber hervor, dass eine solche feingranulare Untergliederung für deutsche KMU aufgrund ihres offenbar i. d. R. geringen Reifegrads des Informationssicherheitsbewusstseins (ISA) derzeit nicht passend ist. Vielmehr sprechen die erkannte große KMU-Heterogenität und der noch deutlich ausbaufähige Awareness-Reifegrad gegen eine kurzfristige Diversifikation, denn für die angedachten Tätigkeits-, Sicherheits- bzw. Kompetenzprofile konnte keine psychologische Relevanz ermittelt werden [11]. Damit wurde deut-

lich, dass in KMU verstärkt für alle Mitarbeitenden eine Bewusstseinsbildung (awareness raising) für Informationssicherheit stattfinden sollte. Der Aspekt der Profile wurde im Projekt separiert, durch eine Online-Umfrage untersucht und als Report 1 [51] veröffentlicht; hier konnten sieben übergreifende Tätigkeitsbereiche definiert werden, für die bei gestiegenem Awareness-Reifegrad weiter spezifizierte Lernmaterialien entwickelt werden könnten. Für weitere Ausführungen siehe auch [61].

Die zweite tiefenpsychologische Befragung (Studie 2) [29] hatte zum Ziel, die entwickelten und bereits erprobten sowie verbesserten analogen Lernszenarien (Serious Games) abschließend zu evaluieren und diese Erkenntnisse für die Erstellung der finalen Versionen zu nutzen. Es konnten zu diesem Zeitpunkt sechs der sieben entwickelten analogen Serious Games evaluiert werden [29] (s. a. [33] [49]):

- Sicher zuhause wohnen & arbeiten (Themen „Homeoffice", „Smart Home" sowie generell private Sicherheit im eigenen Haus bzw. der eigenen Wohnung)
- Die 5 Phasen des CEO Fraud (Thema „Chef-Betrug", s. auch [57])
- Kundendaten sicher managen in Cloud & Co. (Themencluster aus „Passwort", „Kundendaten" und „Cloud Security")
- Mobile Kommunikation, Apps & Co. (Thema „Risiken und deren Abwehr bei der Nutzung mobiler Apps")
- Cyber Pairs (Themencluster „Angriffsvektoren bei Wirtschaftsspionage", „Cyber Crime", „Social Engineering & Co.")
- Informationsklassifizierung (Themen „Klassifizierung" bzw. „Verwendungszweck von Dokumenten, Daten, Informationen").

Laut Zwischenfazit der Studie 2 [29] ist bei allen Gemeinsamkeiten und insbesondere in Bezug auf die notwendige Sicherheitskommunikation kein KMU wie das andere. Es werden unter anderem hinsichtlich Branche, Services bzw. Produkte, Eigentumsverhältnisse, Historie, Zusammensetzung der Belegschaft, Auftritt und Kommunikation große kulturelle Unterschiede gewahr, die nicht nur die Organisation selbst betreffen, sondern auch deren Sicherheitskultur [29]. Es zeigte sich zudem, dass in den befragten deutschen KMU deutlich ausdifferenziertere Sicherheitskulturen existieren als in Großunternehmen. Erste Überlegungen zu einem „Modell Sicherheitskultur KMU" wird in [33] gegeben und wird ausführlich im derzeit erarbeitenden Report 2 diskutiert, der ab September 2023 auf der Projektwebseite [7] zum Download bereitstehen wird.

Wir müssen somit von einer sehr deutlichen sicherheitskulturellen Bandbreite in den deutschen KMU ausgehen. Damit einher existiert eine deutlich unterschiedliche Ausprägung des Awareness-Reifegrads in den Unternehmen. Vor diesem Hintergrund scheint eine Awareness-Patentlösung im Sinne von „One-size-fits-all" für alle Ausprägungen von Sicherheitskultur im gesamten KMU-Spektrum praktisch unmöglich [29] und wird von der internationalen wissenschaftlichen Literatur [62] bestätigt. Jedoch gibt es bei den im Projekt „ALARM Informationssicherheit" entwickelten analogen Serious Games einen großen Vorteil: 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 anzupassen [29].

Als Fazit der Evaluation (Studie 2 [29]) resultierte, dass die analogen erlebnisorientierten Lernszenarien (Serious Games) des Projektes „ALARM Informationssicherheit" mit den verbundenen Simulationen anspruchsvolle, vitalisierende Awareness-Werkzeuge für KMU darstellen. Diese analogen Serious Games für KMU schaffen es, die Überwältigung der Mitarbeitenden mit dem oft abstrakten Thema Informationssicherheit auf ein angemessenes Maß zu reduzieren sowie deren Angst vor Risiken und ggf. vor dem Versagen zu nehmen. Die Mitarbeitenden können sich angstfrei öffnen, ihre Erfahrungen teilen und Dinge nachfragen, erringen damit eine Balance zu diesem so „störenden Thema" Informationssicherheit, lernen es für ihren konkreten Arbeitsplatz einzuordnen. Das ist die gewollte Erzeugung von Awareness-/Sensibilisierungs-Maßnahmen: Achtsam werden und bleiben. Deshalb ist es so wichtig, ein Format zu haben, wie es unsere analogen Serious Games darstellen, die kurz für 15 Minuten oder lang bis zu einer Stunde eingesetzt werden können.

Vor allem die Stationen „Sicher zuhause wohnen & arbeiten" und „Cyber Pairs" sowie „Mobile Kommunikation, Apps & Co." konnten bei der Evaluation als sehr gute Kommunikationsbeschleuniger überzeugen, sodass die Teilnehmenden in einen wertvollen Diskurs zum Thema Informationssicherheit involviert wurden [29]. Auch die anderen analogen Serious Games funktionieren ähnlich, jedoch nach der zweiten Studie [29] nicht in jedem Umfeld gleich gut. Insbesondere das Lernszenario „Informationsklassifizierung" wurde aufgrund dieser Evaluation noch einmal stark verändert, vor allem da in den meisten KMU eine Klassifizierung (noch) nicht als Standardprozess etabliert ist [29]. Unsere Erkenntnis war: Kein analoges Lernszenario funktioniert überall gleich gut und eine exakte Passung des jeweiligen Serious Games zu definieren, wird durch die große kulturelle Heterogenität im deutschen KMU-Umfeld erschwert. Eine zielgruppenorientierte Ausdifferenzierung der Lernszenarien konnte derzeit ebenfalls nicht empfohlen werden, da dazu der Awareness-Reifegrad in den deutschen KMU i. d. R. noch erhöht werden muss. Mit den im Projekt „ALARM Informationssicherheit" entwickelten Lernszenarien und Materialien sollte daher erst einmal ein Basislevel an Awareness für Informationssicherheit in KMU geschaffen und nachhaltig gesichert werden. Spezialisierungen sind weiteren partizipativen Informationssicherheitsprojekten vorbehalten.

Aus der zweiten Studie haben wir allerdings erkannt,

dass „Security Awareness“ von den Befragten als wichtiger Baustein der Informationssicherheit betrachtet wird und die gamifizierte Entwicklung generell äußerst vitalisierend wirkt. Im Spielen waren alle Teilnehmenden aus KMU motiviert, gut gelaunt und zugleich ernsthaft und konzentriert [29]. Auch in der von uns besonders befürworteten Nachbetrachtung während der Gruppendiskussionen trugen alle Teilnehmenden zu einem produktiven Feedback bei. Somit konnten wir schlussfolgern, dass der Ansatz, Awareness mithilfe von Gamification auf ein Niveau zu heben, das Einbindung schafft und die Sensibilisierungsleistung lerntheoretischer Ansätze deutlich übersteigt, gut funktionierte [28]. Der Austausch beim Spielen wurde mehrheitlich positiv beurteilt, vor allem dann, wenn sich in Selbstorganisation Kleingruppen oder Paare bildeten und synchron zu den jeweils anderen sehr persönlich miteinander diskutierten [29]. In diesem Fall müssen die moderierenden Personen allerdings unbedingt die zur Verfügung stehende Zeit im Blick behalten. Immer wieder wurde sehr positiv bewertet, dass Gespräche über „Situationen aus dem wahren Leben“ durch die Spiele angeregt werden [29]. Das zeigt, dass unsere Serious Games eine Art Simulation realer Arbeits- und Alltagsszenarien darstellen. Auch der Bezug zur Informationssicherheit im eigenen Privatleben wurde offensichtlich gut und klar verdeutlicht.

Die erfolgreiche Evaluation der im Projekt „ALARM Informationssicherheit“ entwickelten analogen Serious Games für Security Awareness in KMU ist somit gegeben – sie schaffen einen sozialen Raum und liefern den Anwendenden die Dramaturgie für den konkreten Sensibilisierungsprozess gleich mit. Trotzdem musste die Studie 2 [29] darauf hinweisen, dass die Awareness-Maßnahmen wirkungslos bleiben, wenn die analoge/digitale Autonomie der Mitarbeitenden als interne „lebende Firewall“ nicht integrativ mitgefördert wird. Mitarbeitende, denen nicht zugetraut wird, sich verantwortungsbewusst zu verhalten, fühlen sich entmündigt [29]. Sicherheit durch Unterbindung von solcher Entscheidungsfreiheit kann zu Reaktanz und diese wiederum zu neuen Sicherheitsvorfällen im Unternehmen führen. Stattdessen benötigen wir jedoch Resilienz. “Resilienz ist die Fähigkeit, Veränderungen in der Umgebung aufzunehmen und sich an diese anzupassen (ISO/IEC-Norm 22300), dabei spielt das Risikomanagement eine zentrale Rolle (ISO/IEC-Norm 31010)“ [63]. Bereits in früheren Projekten zeigte sich die große Bedeutung der Risikobeurteilung für alle Mitarbeitenden bzw. das Risikomanagement als ein zentraler Aspekt für die Führungskräfte. Auch hierfür hatten wir bereits ein analoges Serious Game entwickelt [44]. Security Awareness bzw. Sensibilisierung ist somit „Sozialarbeit“ in KMU [29] und dazu wird das gesamte Management als Vorbild benötigt.

Diese nun vorliegende dritte Studie des Projekts „ALARM Informationssicherheit“ ergänzt die beiden ersten durch sehr konkrete Antworten auf viele uns gestellter Fragen, die wir immer wieder bei der Durchführung von Sensibilisierungsveranstaltungen hören. Sie soll die Moderatorinnen und Moderatoren bzw. Multiplikatorinnen und Multiplikatoren von Security-Awareness-Maßnahmen, aber auch Geschäftsführende als Top-Management und IT- und Sicherheitsfachkräfte dabei unterstützen, eine angemessene Kommunikation in den Unternehmen aufzubauen, um Sensibilisierung und Schulungen zu Informationssicherheits- und Datenschutzthemen erfolgreich zu planen, durchzuführen und zu evaluieren. Diese Studie 3 behandelt mit den Moderationsbriefings bzw. zahlreichen Hinweisen und Tipps zu den analogen Lernszenarien die folgenden Aspekte:

- Die Hintergründe Awareness, Reifegrad und Sicherheitskultur,
- das Material der analogen Serious Games,
- die Spielvorbereitung der einzelnen analogen Serious Games,
- das jeweilige Ziel und die didaktische Intention der einzelnen Spiele,
- die Stories inklusive Spieldynamik der einzelnen Lernszenarien,
- Tipps für die Moderation,
- Goldene Regeln für die Teilnehmenden,
- mögliche Fragen und
- die Lösungen der jeweiligen analogen Lernszenarien.

Inzwischen gehört Security Awareness zwar formal zu den gesetzten Bestandteilen der Geschäftsprozesse und Compliance-Definitionen von Unternehmen, aber es wird nicht zwingend von allen Beteiligten gelebt. Die erfolgreiche Sensibilisierung der Mitarbeitenden für mehr Informationssicherheit ist jedoch unbestreitbar ein Erfolgsfaktor für KMU. Diese Studie 3 ist daher als Leitfaden für die KMU zu verstehen, somit ein praktischer Ratgeber zur Selbsthilfe.

Darüber hinaus werden die erkannten Erfolgsfaktoren mit nachhaltiger Wirkung von Security-Awareness-Maßnahmen zusammengefasst. Die Sicherheitskultur ist in KMU auszubauen, die Geschäftsführenden sind als Unterstützung zu gewinnen und sollten die systemische Kommunikation hinsichtlich Informationssicherheit ausbauen. Die Führungskräfte müssen ihre Rolle/Funktion als Vorbilder verstehen lernen, Multiplikatorinnen und Multiplikatoren für Informationssicherheit und Awareness erkennen und einsetzen sowie Zeit-Ressourcen für die Beschäftigten für Sensibilisierungsmaßnahmen zur Verfügung stellen. Es sind zielführende Methoden mit hohem Synergiefaktor einzusetzen, die persönlichen Vorteile für alle Zielgruppen zu vermitteln und dabei eine klare und authentische, vor allem nicht technische Ansprache zu wählen sowie, mit steigendem Reifegrad, zielgruppenorientiert zahlreiche verschiedene Kanäle der Kommunikation einzusetzen.

Der notwendige Mix über zahlreiche Kanäle wird auch international bestätigt: „Die Übermittlung derselben

Botschaft auf verschiedene Arten hat die Einstellung der Mitarbeiter zur Bedeutung von Sicherheitsmaßnahmen wirksamer verändert als die nur einmalige Übermittlung“ [64]. Ebenso ist auch international zu erkennen, dass eine Überforderung der Mitarbeitenden mit zu vielen technischen Informationen einen negativen Effekt haben kann [64]: Es ist besonders wichtig, das Training ansprechend und interessant zu gestalten, denn es fördert die Teilnahmebereitschaft, treibt die Mitarbeitenden zu mehr Selbstentwicklungsaktivitäten, unterstützt das (erlernte) Wissen durch Peer-to-Peer-Interaktion schneller zu verbreiten und verringert die inzwischen auftretende „Sicherheitsmüdigkeit“ der Menschen. Weltweit bleiben Aufklärung, Schulung und Sensibilisierung für Informationssicherheit die Ansätze zur Änderung des Sicherheitsverhaltens [65]. Doch das Sicherheitsverhalten ist ein sehr komplexes, mehrdimensionales, nicht-lineares Konstrukt, wozu es weiterer Forschung bedarf. Mit etlichen Modellen versucht man aktuell, sich dieses Konstrukt zu erschließen (siehe z. B. [66] [67] [62]). In den drei Studien unseres Projektes wird darauf hingewiesen, dass eine reine Wissensvermittlung inzwischen als gescheitert gilt (s. a. [24] [43] [67]), weshalb gerade im Projekt „ALARM Informationssicherheit“ neue Wege gegangen und erlebnisorientierte Lernszenarien bzw. Serious Games entwickelt wurden.

5.2 Unsere Erkenntnisse aus den drei Studien für deutsche KMU

Das Projekt „ALARM Informationssicherheit“ hat seine Ziele umfangreich erfüllt und stellt in der Praxis erprobte hervorragende Materialien für die Sensibilisierung von Mitarbeitenden in KMU kostenfrei über die Webseite für mehr Informationssicherheit in KMU zur Verfügung (s. [7]). Die analogen und digitalen Serious Games sowie weitere Materialien wie z. B. dazu passende niederschwellige Sicherheitskonzepte beinhalten auch Anleitungen und Hinweise für die konkrete interne Umsetzung von diesem didaktisch aufbereiteten Mix an Sensibilisierungsmaßnahmen in deutschen KMU.

Unabhängig von dem erfolgreichen Projektabschluss mit allen finalen Ergebnissen im September 2023 bleiben weitere Aktivitäten gefragt: So ist eine gezielte breitenwirksame Bekanntmachung und Nutzung dieser existierenden qualitativ und didaktisch hochwertiger Materialien für die Sensibilisierung von Mitarbeitenden angebracht, um den Transfer in die KMU zu stärken. Darüber hinaus sollten wir uns dem Thema „Sicherheitskultur“ in deutschen KMU stärker widmen. Denn eine sichere digitale Transformation im deutschen Mittelstand kann nur durch kontinuierliche Verbesserung der Sicherheitskultur infolge von Kompetenzerhöhung in Bezug auf Cyber-Security geschehen. Dies betrifft gerade auch die Geschäftsführenden bzw. das Management, denn Informationssicherheit ist nicht nur Chef(in)-Sache, sondern ein besserer Security-Awareness-Reifegrad, als derzeit im KMU-Durchschnitt vorhanden, ist Voraussetzung für den Erfolg der derzeitigen Digitalisierung.

Ein immer wiederkehrender Aspekt – sei es in unseren Trainings, sei es in den einschlägigen Normen [46] und Standards [45 oder in der internationalen wissenschaftlichen Literatur – ist die Bedeutung der unterstützenden Rolle und Vorbildfunktion des Top-Managements bzw. der Geschäftsführung und ebenso der Führungskräfte. Damit ist die Erhöhung des IT- und Cybersicherheitsniveaus im Mittelstand durch sukzessive Steigerung der Security Awareness bei Entscheiderinnen und Entscheidern und dem Management mit entsprechender Weitergabe der Awareness-Skills top down an die Mitarbeitenden viel stärker notwendig als bislang berücksichtigt. Managerinnen und Manager als Security-Vorbilder zu entwickeln, setzt aber ein methodisches Verständnis von Security Awareness voraus sowie die Kompetenz, Cyber-Security und Awareness verständlich, d. h. bildhaft, leicht und nachvollziehbar, zu kommunizieren. Wissen in KMU, Handwerksbetrieben und Start-ups über die Gefahren der digitalen Welt im Allgemeinen ist dabei nicht allein ausreichend, um nachhaltige Security Awareness zu sichern, denn Wissen muss über emotionale und systemische Kompetenzen ergänzt werden, um einen ausreichenden Security-Awareness-Reifegrad zu erzielen. Hierzu gehört ein wesentlich besseres Verständnis als wir derzeit haben, weshalb auch hier weitere Forschung notwendig ist.

Nach unserer anwendungsorientierten und praktischen Erfahrung mit dem Projekt „ALARM Informationssicherheit“ muss ein besseres Verständnis in deutschen KMU vor allem in Bezug auf Marketingmittel in der Awareness für Informationssicherheit geschaffen werden. Es sollten somit einprägsame Geschichten (Narrative, Story Telling), Imagination, Metaphern zur Reduzierung der Themenkomplexität sowie die Vereinfachung von Sicherheitskommunikation dem Management bekannt sein. Vor allem plädieren wir für eine systemische Kommunikation mit insbesondere „diskursiver Didaktik“. Dies bedeutet, das Prinzip „Talking Security“ in den KMU-Geschäftsprozessen zu erhöhen und damit eine weitere Prävention vor Cyberangriffen aufzubauen, nämlich die (freie) Sprechfähigkeit in Bezug auf Cyber-Security, ihre Risiken und die entsprechende Verteidigung (Defense) zu verbessern.

Dies bedeutet gleichzeitig, dass das Wissen in KMU, Handwerksbetrieben und Start-ups über Handlungsmöglichkeiten in allen Teilbereichen der Cybersicherheit, sei es Prävention, Detektion oder Reaktion, erhöht werden muss. Da deutsche KMU mit Ressourcen für Informationssicherheit zu kämpfen haben, muss deutlich gemacht werden, dass eine systemische Beratung der Geschäftsführung und der Führungskräfte mit wirksamen Tools notwendig ist. Mit „wirksamen Tools“ meinen wir einfache, bildlich aufbereitete und haptisch begreifbare gamifizierte Materialien spezifiziert für das Management, sodass deren Risikobeurteilung der KMU-Lage, Prioritätensetzung der Maßnahmen

und Führung als Sicherheitsvorbild gestärkt, nachvollziehbar eingesetzt und akzeptiert wird.

Ziel muss sein, die Handlungskompetenz in allen Teilbereichen der Cybersicherheit in KMU, Handwerksbetrieben und Startups durch Demonstration und Transformation von Sicherheitskommunikationsmethoden zu erhöhen. Das Top-Management und die Führungskräfte müssen fähig sein, ihre begründete Einschätzung der betrieblichen Sicherheitslage adäquat und verständlich top down an die Mitarbeitenden weitergeben können. Vielleicht können zudem „Ambassador-Konzepte" von Awareness und Sicherheitskommunikation so umgesetzt werden, dass Mitarbeitende zu „Awareness-Botschafterinnen und -Botschaftern" heranreifen können.

Wir schlussfolgern,

- dass ein erster Schritt die Etablierung von Moderatorinnen und Moderatoren innerhalb eines KMU sein könnte. Sie hätten die Aufgabe, praxisbezogene, bildhafte, narrative Methoden und Formate einzusetzen, um damit relevante, aber abstrakte Themen zu veranschaulichen und so erhebliche Barrieren der Informationssicherheit innerhalb des KMUs zu beseitigen;
- dass als ein zweiter Schritt die Etablierung einer anerkannten Ausbildung von Moderatorinnen und Moderatoren notwendig wird, seien sie intern im Unternehmen rekrutiert oder seien es solche aus Beratungsunternehmen (Multiplikatoren). Die Ausbildung soll die Moderatorinnen und Moderatoren bzw. Multiplikatorinnen und Multiplikatoren befähigen, die Cyber-Security-Themen aus den IT-Zusammenhängen so zu entkoppeln, dass sie für alle verständlich werden und eine tatsächlich begreifbare Sicherheitskommunikation aufgebaut werden kann;
- dass in einem dritten Schritt die Etablierung einer anerkannten Zertifizierung von Moderatorinnen und Moderatoren bzw. Multiplikatorinnen und Multiplikatoren von Bedeutung ist, um eine Nachhaltigkeit zu erzielen.

5.3 Ausblick für weitere anwendungsorientierte Forschung und praktische Umsetzung in KMU

Der Einsatz sicherer digitaler Prozesse, digitaler Technologien und digitaler Geschäftsmodelle und damit auch die Sicherung und Erhöhung der Wettbewerbs- und Innovationsfähigkeit des deutschen Mittelstands ist ein MUSS für Deutschland, für den Wohlstand der Bürgerinnern und Bürger, für die Weiterentwicklung der Unternehmen und für die Behörden als Mittelgeber für neue Förderungen. Nach unseren Erfahrungen in diversen Sicherheitsprojekten mit dem Fokus auf „den Faktor Mensch" und mit unterschiedlichsten Zielgruppen und Akteurinnen und Akteuren ist dies durch Visualisierung, Narration, Reduzierung der Komplexität und gleichzeitigem Aufbau eines Verständnisses komplexer Bedingungen und Zusammenhänge möglich. Das würde vermutlich auch die Menschen näher an die Technologien der Zukunft heranrücken lassen: Partizipativ informiert sein, eingebunden diskutieren und verstehen, aktiv handlungsfähig sein und auf Augenhöhe involviert sein.

Eventuell wird es nicht jedes KMU aus eigener Kraft stemmen können. Daher sind auch Transferstrukturen mit anderen Akteurinnen und Akteuren der IT- und Cybersicherheit zu etablieren, in denen die entwickelnden gamifizierten Methoden für Mitarbeitende und neu zu entwickelnden Beratungstools für das Top-Management mit zertifizierten Multiplikatorinnen und Multiplikatoren von spezialisierten Beratungsunternehmen weiterentwickelt oder an diese zur praktischen Nutzung innerhalb etablierter Kundenbeziehungen mit KMU übergeben werden. Technologische, organisatorische und arbeitsgestaltende Kompetenzen der IT- und Cybersicherheit sollen damit erhöht sowie Sicherheit von und Vertrauen in (Anbieter-/Anwender-) Informations- und Kommunikationssysteme einschätzbar werden. Dazu müssen die Zusammenhänge von IT- und Cybersicherheit und Datenschutz thematisiert und in nachvollziehbare Geschichten und Bilder übersetzt werden. Generell ist im Zuge der Digitalisierung zu vermerken, dass sowohl Beauftragende, Anbietende und Betreibende von Plattformen als auch Entwicklerinnen und Entwickler von digitalen Lösungen (Online-Services) die Nutzenden der Systeme im Fokus haben sollten, seien es Mitarbeiterinnen und Mitarbeiter, Verbraucherinnen und Verbraucher oder allgemein Bürgerinnen und Bürger (s. auch [68]).

Trotz der absoluten Erfolgsgeschichte des Projekts „ALARM Informationssicherheit" mit all seinen Beteiligten sehen wir durchaus verbleibende Defizite. Diese liegen nach den bisherigen Erkenntnissen des Projekts in deutschen KMU in drei Bereichen:

- Die Bereitstellung von qualitativ und didaktisch hochwertigen Sensibilisierungsmaterialien für Mitarbeitende in KMU ist nicht ausreichend, damit KMU diese tatsächlich innerbetrieblich nutzen. Vielmehr müssen KMU dazu stärker „an die Hand genommen" werden, damit der Transfer zur nachhaltigen Nutzung gelingt.
- Dies bedeutet zum einen, dass Moderatoren/Moderatorinnen für die Sensibilisierungsmaßnahmen innerhalb der KMU ausgebildet werden sollten („Awareness Berater/Beraterinnen"). Diese können intern im KMU rekrutiert werden oder extern über Beratungsfirmen erfolgen. Die Qualität der Moderation hängt wiederum von einer guten Ausbildung ab, die über eine Zertifizierung sichergestellt werden sollte.
- Des Weiteren sind ein entscheidender Faktor für die erfolgreiche Sicherheitskommunikation das Top-Management (Geschäftsführende) und die Führungskräfte innerhalb der KMU. Hier können vor allem Beratungsunternehmen eine entscheidende Transferfunktion übernehmen. Allerdings benötigt eine Beratung/ein

Coaching andere Materialien für Führungskräfte als die bislang entwickelten Sensibilisierungsmaßnahmen für Mitarbeitende.

Damit ist die Bewilligung weiterer anwendungsorientierter Forschungsprojekte im Bereich Informationssicherheit/ Cyber-Security spezialisiert auf das Top-Management in deutschen KMU notwendig.

Prof. Dr. rer. nat. Margit C. Scholl, TH Wildau

August 2023

Literatur

[1] https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf, Zugriff: 28.07.2023

[2] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022, Zugriff: 28.07.2023

[3] https://presse.gothaer.de/pressreleases/gothaer-kmu-studie-2022-deutscher-mittelstand-aus-ueberzeugung-nachhaltig-3174479, Zugriff: 28.07.2023

[4] https://netzpalaver.de/2023/05/25/die-kosten-fuer-cyberversicherungen-steigen-drastisch/, Zugriff: 28.07.2023

[5] https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.item-738a133628e04cb9ff6114486f1d9964.html, Zugriff: 28.07.2023

[6] https://cybersecurityventures.com/ransomware-report-2021/, Zugriff: 28.07.2023

[7] https://alarm.wildau.biz/, Zugriff: 09.08.23

[8] Europäische Kommission (Ed.) (2015). Benutzerleitfaden zur Definition von KMU. Luxemburg: Amt für Veröffentlichungen der Europäischen Union

[9] Krämer, W. (2003). Mittelstandsökonomik. München: Vahlen

[10] Gesamtverband der Deutschen Versicherungswirtschaft e. V. (Ed.) (2021). Cyberrisiken im produzierenden Gewerbe. Berlin

[11] Pokoyski, D., Matas, I., Haucke, A., & Scholl, M. (2021). Qualitative Wirkungsanalyse Security Awareness in KMU. Projekt „ALARM Informationssicherheit“. In: Scholl, M. (Hrsg.) [online] Wildau: Technische Hochschule Wildau, p.72. Available at: https://alarm.wildau.biz/.

[12] known_sense (Hrsg.) (2016). Security Awareness Framework. Köln

[13] ISO/IEC 27001: 2013 (2013). Berlin: Beuth

[14] https://www.buzer.de/Krankenhauszukunftsgesetz.htm, Zugriff: 28.07.2023

[15] https://www.is-its.org/it-security-blog/wie-schuetzt-man-kritische-infrastrukturen-kritis-vor-cyberangriffen, Zugriff: 28.07.2023

[16] DIN SPEC 27076 (2023). Berlin: Beuth

[17] https://netzpalaver.de/2023/05/02/wie-kleine-und-kleinstunternehmen-im-rahmen-der-spec-27076-security-awareness-umsetzen-koennen/, Zugriff: 28.07.2023

[18] https//s3.eu-central-1.amazonaws.com/7003001237.pdf. Zugriff: 28.07.2023

[19] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html, Zugriff: 28.07.2023

[20] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html, Zugriff: 28.07.2023

[21] https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/kampagne_node.html, Zugriff: 28.07.2023

[22] https://www.bakoev.bund.de/DE/02_Themen/Informationstechnik/sicher_gewinnt/sicher_gewinnt.html, Zugriff: 28.07.2023

[23] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Trainigskoffer/Trainingskoffer.html, Zugriff: 28.07.2023

[24] Helisch, M. & Pokoyski, D. (Hrsg.) (2009). Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung / Security Awareness – New ways to successfully raise employee awareness. Wiesbaden: Springer Vieweg.

[25] Imdahl, I. (2006) Wertvolle Werbung. In: rheingold (ed.) (2006). rheingold-Newsletter, N. 1. Köln

[26] https:// www.known-sense.de/Methoden, Zugriff: 04.08.2023

[27] known_sense, T-Systems International (Hrsg.) (2010). Tiefenpsychologische Konzeptanalyse mySecurity & Privacy Box bei T-Systems International. Köln

[28] https://www.known-sense.de/newpagec02b9c19, Zugriff: 04.08.2023

[29] Pokoyski, D. & Haucke, A. (2022). Enabling vs. Entmündigung – Qualitativer Konzepttest analoger Security Awareness-Lernszenarien für KMU im Projekt »ALARM Informationssicherheit«. In: Scholl, M. (Hrsg.), [online] Wildau: TH Wildau. Available at: https://alarm.wildau.biz/static/c0e4d00beefe1dc5fac9b50b6087265f/studie-2-master-final.pdf.

[30] http://s522854922.online.de/SecurityArenaThemenueberblick.pdf, Zugriff: 28.07.2023

[31] Kolarow, J. (2019). Entwicklung eines analogen Lernformates für die Schulung von Compliance-Inhalten unter Berücksichtigung lernpsychologischer Faktoren, Masterthesis. Köln: Rheinische Fachhochschule Köln

[32] www.known-sense.de/security-arena, Zugriff: 28.07.2023

[33] 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. 36. AKWI Jahrestagung 2023. Erweiterung für die INFORMATIK 2023

[34] Prott, F., Küchler, U., Schuktomow, R. & Scholl, M. (2022), Serious Games als Lernmethode zur Steigerung der Informationssicherheit. In: AKWI-Tagungsband zur 35. AKWI-Jahrestagung (2022), S. 325–334

[35] Ypsilanti, A., Vivas, A.B., Räisänen, T., Viitala, M., Ijäs, T. & Ropes, D. (2014). Are Serious Video Games Something More than a Game? A Review on the Effectiveness of Serious Games to Facilitate Intergenerational Learning. Education and Information Technologies, 19, S. 515–529

[36] https://www.known-sense.de/wanted-security-giveaways, Zugriff: 28.07.2023

[37] Sasse, M. A., Hielscher, J., Friedauer, J., & Peiffer, M. (2022). Warum IT-Sicherheit in Organisationen einen Neustart braucht / Why IT security in organizations needs a fresh start. Federal Office for Information Security (BSI) (Hrsg.) (2022): Proceedings of the 18. Deutscher IT-Sicherheitskongress des BSI / 18th German IT Security Congress of the BSI, Februar 2022.

[38] Scholl, M., & Schuktomow, R. (2021). The Current State of „Information Security Awareness“ in German SMEs. International Journal of Emerging Technology and Advanced Engineering (IJETAE), [online] 11(12), pp.151–163. Available at: https://ijetae.com/files/Volume11Issue12/IJETAE_1221_16.pdf.

[39] Dang-Pham, D., Kautz, K., Hoang, A. P., & Pittayachawan, S. (2022). Identifying information security opinion leaders in organizations: Insights from the theory of social power bases and social network analysis. Computers & Security, 112, 102505.

[40] BSI (2022). Die Lage der IT-Sicherheit in Deutschland. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=5, Zugriff: 19.07.23.

[41] DIHK—Deutscher Industrie- und Handelskammertag e. V. (Hrsg.) (2022). Zeit für den digitalen Aufbruch: Die IHKUmfrage zur Digitalisierung/Time for the digital awakening. The IHK survey on digitization.

[42] Zerr, K. (2007). Security-Awareness-Monitoring. DuD Datenschutz und Datensicherheit 31. Wiesbaden: Springer Gabler.

[43] Bada, M., Sasse, A.M., & Nurse, J.R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? ArXiv, abs/1901.02672

[44] Scholl, M., Gube, S. and Koppatz, P., 2021. Development of Game-Based Learning Scenarios for Social Engineering and Security Risk Management for SMEs in the Manufacturing Industry. Journal of Systemics, Cybernetics and Informatics, [online] 19(2), pp. 51–59. Available at: http://www.iiisci.org/journal/sci/FullText.asp?var=&id=ZA516ND21.

[45] a) BSI —Bundesamt für Sicherheit in der Informationstechnik (2017). BSI-Standards 200-1 bis 200-4. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html, Zugriff: 09.08.2023

b) BSI —Bundesamt für Sicherheit in der Informationstechnik (2020). BSI-Kompendium, Baustein ORP.3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/02_ORP_Organisation_und_Personal/ORP_3_Sensibilisierung_und_Schulung_Editon_2022.pdf?__blob=publicationFile&v=3, Zugriff: 09.08.2023

[46] a) ISO/IEC 27000:2018(E), Information technology — Security techniques — Information security management systems— Overview and vocabulary. INTERNATIONAL STANDARD ISO/IEC 27000, fifth edition 2018-02.

b) ISO/IEC 27001:2017. Berlin: Beuth, 2017.

[47] a) Scholl, M., & Ehrlich, E.-P. (2020). Informationssicherheitsbeauftragte: Aufgaben, notwendige Qualifizierung und Sensibilisierung praxisnah erklärt. Frankfurt am Main: Buchwelten-Verlag.

b) Scholl, M., & Ehrlich, E.-P. (2020). Information Security Officer: Job profile, necessary qualifications, and awareness raising explained in a practical way. Frankfurt am Main: Buchwelten-Verlag.

[48] Alotaibi, S., Furnell, S., & He, Y. (2023). Towards a Framework for the Personalization of Cybersecurity Awareness. In: Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham. https://doi.org/10.1007/978-3-031-38530-8_12.

[49] Scholl, M. (2023). Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. URI: https://hdl.handle.net/10125/103369. ISBN: 978-0-9981331-6-4 (CC BY-NC-ND 4.0), pages 6058-6067.

[50] Scholl, M. (2021). Foreword with an Introduction to and Summary of the Study “Added Value for SMEs” (Translation). Vorwort zur Qualitative Wirkungsanalyse Security Awareness in KMU Tiefenpsychologische Grundlagenstudie im Projekt »Awareness Labor KMU (ALARM) Informationssicherheit«. DOI: 10.13140/RG.2.2.21236.88961

[51] 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. Available at: https://alarm.wildau.biz/static/20b6d15448c0ba23729e0f45daa20650/alarm-informationssicherheit-report-1.pdf.

[52] Kävrestad, J., Fallatah, W., Furnell, S. (2023). Cybersecurity Training Acceptance: A Literature Review. In: Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham, pp. 53-63. https://doi.org/10.1007/978-3-031-38530-8_5 .

[53] Fertig, T., Schütz, A., & Weber, K. (2022). Automated Measuring of Information Security Related Habits. Proceedings of the 55th Hawaii International Conference on System Sciences | 2022. URI: https://hdl.handle.net/10125/80267. ISBN: 978-0-9981331-5-7 (CC BY-NC-ND 4.0), pages 7702-7711.

[54] Ogbanufe, O. (2020). “Information Security Is Not Really My Job”: Exploring Information Security Role Identity in End-Users. Proceedings of the 53rd Hawaii International Conference on System Sciences 2020. URI: https://hdl.handle.net/10125/64263. ISBN: 978-0-9981331-3-3 (CC BY-NC-ND 4.0), pp 4256-4263.

[55] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behav. Inf. Technol., vol. 33, no. 3, pp. 237_248.

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

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

[58] sosafe: Human Risk – Review 2023. Die europäische Cyber-Bedrohungslage: Experteneinblicke und Strategien, https://sosafe-awareness.com/de/ressourcen/reports/human-risk-review/, Zugriff 13.07.2023.

[59] Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. Proceedings of the 51st Hawaii International Conferenceon System Sciences 2018. URI: http://hdl.handle.net/10125/50524. ISBN: 978-0-9981331-1-9 (CC BY-NC-ND4.0), pages 5085-5094.

[60] Farshadkhah, S., & Stafford, T. (2019). The Role of “Eyes of Others” in Security Violation Prevention: Measures and Constructs. Proceedings of the 52nd Hawaii International Conference on System Sciences 2019. URI: https://hdl.handle.net/10125/59927. ISBN: 978-0-9981331-2-6 (CC BY-NC-ND 4.0), pages 4895-4903.

[61] von Tippelskirch, H., & Scholl, M. (2022). 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, [online] 10(1), pp.787–795. Available at: https://infonomics-society.org/jitst/published-papers/volume-10-2022/.

[62] Topa, I., & Karyda, M. (2023). Addressing Organisational, Individual and Technological Aspects and Challenges in Information Security Management: Applying a Framework for a Case Study. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. URI: https://hdl.handle.net/10125/102687. ISBN: 978-0-9981331-6-4 (CC BY-NC-ND 4.0), pages 470-479.

[63] Homepage Jutta Heller, https://juttaheller.de/resilienz/resilienz-abc/definition-organisationale-resilienz/. 18.07.2023.

[64] Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. IEEE Access, 10, 132132-132143.

[65] Nwachukwu, U., Vidgren, J., Niemimaa, M., & Järveläinen, J. (2023). Do SETA Interventions Change Security Behavior?: A Literature Review. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. URI: https://hdl.handle.net/10125/103396. ISBN: 978-0-9981331-6-4 (CC BY-NC-ND 4.0), pages 6300-6309.

[66] Jaeger, L. (2018). Information security awareness: literature review and integrative framework. Proceedings of the 51st Hawaii International Conferenceon System Sciences 2018. URI: http://hdl.handle.net/10125/50482. ISBN: 978-0-9981331-1-9 (CC BY-NC-ND4.0), pages 4703-4712.

[67] Schütz, A., & Fertig, T. (2023). The Forgotten Model–Validating the Integrated Behavioral Model in Context of Information Security Awareness. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. URI: https://hdl.handle.net/10125/103462. ISBN: 978-0-9981331-6-4 (CC BY-NC-ND 4.0), pages 6841-6850.

[68] Ruiz Ben, E., & Scholl, M. (2023). Challenges Posed by the Digital Transformation Paths of the Online Access Act in Germany: Implementation and the Need to Raise Awareness. In J. Liebowitz, Pivoting Government through Digital Transformation (pp. 147–170). Boca Raton: CRC Press [Boca Raton]. Doi: 10.1201/9781003369783-10.

Glossar

Ein praktisches Security Awareness-Glossar von A-Z befindet sich in der Grundlagenstudie ab Seite 66 [11].

Security Awareness und Serious Games

Für die einen ist das „game over“, weil ihr Awareness-Reifegrad eine produktive Nutzung von spielerischen Formaten gar nicht zulässt – andere sind „game lover“, obwohl die Liebe zum Spiel überhaupt nicht notwendig ist, um Gamification als beste Methode zur Bildung nachhaltige Security Awareness zu identifizieren. Der diskursive Aspekt von Sensibilisierung ist und bleibt mithin das wichtigste Mittel, Menschen zu berühren, in Sicherheitsthemen zu involvieren und Beziehung untereinander, zur Organisation und zur Motivation bzw. Absicht herzustellen, die eigene Defense im Sinne von Loyalität und Verantwortung zu adressieren.

Die hier vorliegende dritte Studie des Projekts „ALARM Informationssicherheit“ rundet den Reigen der Projektstudien durch ein „Desk Research“ des Unterauftragnehmers known_sense ab. In der ersten Studie wurden von known_sense tiefenpsychologische Interviews mit den beteiligten Pilotunternehmen durchgeführt, um beispielhaft den Ist-Stand der Informationssicherheit in KMU zu erfassen und daraus die relevanten Themen für die Entwicklung von adäquaten analogen Sensibilisierungsmaterialien zu identifizieren. Diese Erkenntnisse, gepaart mit einer Online-Umfrage, bildeten auch die Grundlage für die Entwicklung der im Gesamtszenario integrativ verzahnten digitalen Lernszenarien und „Vor-Ort-Angriffen“. Das Ziel des Projektes war von Beginn an, dass von der betrieblichen Alltagssituation ausgegangen werden sollte, um eine wissenschaftlich fundierte und gleichzeitig ganz praktische Hilfe für KMU zu entwickeln. KMU sollen die eigene Etablierung von Sensibilisierungsmaßnahmen für die Mitarbeitenden vorantreiben können und so zur Erhöhung der betrieblichen Informationssicherheit und zum Aufbau einer angemessenen KMU-Sicherheitskultur beitragen und letztlich die Erhöhung des Sicherheitsniveaus in deutschen KMU absichern.