ALARM
Awareness Labor KMU
Informationssicherheit

Enabling vs. Entmündigung

Qualitativer Konzepttest analoger Security Awareness-Lernszenarien für KMU im Projekt »ALARM Informationssicherheit«

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

Diese tiefenpsychologische Wirkungsanalyse ist die zweite von insgesamt drei Studien, die im dreijährigen Projekt »Awareness Labor KMU (ALARM) Informationssicherheit« verfasst werden: https://alarm.wildau.biz/

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 – 30.09.2023

Die Studie basiert auf anonymisierten Gruppendiskussionen, Fokusinterviews und Beobachtungen, die von known_sense als Unterauftragnehmer der TH Wildau innerhalb des Projekts mit KMU im Juni und Juli 2022 durchgeführt wurden.

Die Studienergebnisse wurden von known_sense im von Juli bis September 2022 zusammengefasst und mit dem Forschungsteam Scholl der TH Wildau beraten.

Das BMWK hat die Veröffentlichung im November 2022 freigegeben.

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

Verantwortlich für Inhalt und Gestaltung:
known_sense | Jakob-Engels-Str. 39 | 51143 Köln

Feldarbeit | Analyse | Autoren:
Dietmar Pokoyski |
Dipl.-Psychologin Ankha Haucke

Abbildungen:
Abbildungen 1-16 von known_sense
(Abb. 1, 13, 14 inkl. Illustrationen von Shutterstock,
Abb. 15 inkl. Illustrationen von Freepik)
Titelfoto von Shutterstock
Fotos S. 24, 30, 32, 34, 36, 38, 42, 64 von der TH Wildau
(bei den abgebildeten Personen handelt es sich nicht um Probanden/-innen dieser Studie)
Alle weiteren One-Line-Illustrationen von Freepik

Oktober 2022

ISBN 978-3-949639-03-6

Enabling vs. Entmündigung

Qualitativer Konzepttest analoger
Security Awareness-Lernszenarien
für KMU im Projekt »ALARM Informationssicherheit«

Inhaltsverzeichnis

1. Einleitung mit Ausgangslage 7

2. Stichprobe und Untersuchungsdesign 9

2.1 Stichprobe, Test, Moderation, Gruppendiskussionen, Fokusinterviews, Dauer der Befragungen 9

2.2 Quotierung der Probanden/-innen 9

3. Lernszenarien-Methodik bzw. Übersicht Lernszenarien-Testmaterial 13

3.1 Lernszenarien-Methodik 13

3.2 Übersicht Lernszenarien-Testmaterial 15

3.2.1 Sicher zuhause wohnen & arbeiten 15

3.2.2 Kundendaten sicher managen in Cloud & Co. 15

3.2.3 Die 5 Phasen des CEO Fraud 17

3.2.4 Mobile Kommunikation, Apps & Co. 17

3.2.5 Cyber Pairs 19

3.2.6 Informationsklassifizierung 19

3.2.7 Messenger, sichere Übertragung, Verschlüsselung 19

3.2.8 Zusammenfassung Kapitel 3 19

4. Erste Eindrücke aus der Akquise bzw. Feldarbeit 21

5. Atmosphärisches in den KMU im Kontext Unternehmens- bzw. Sicherheitskultur und Kommunikationn 25

5.1 Generelles bzw. Ausprägungen von Unternehmenskultur 25

5.2 Ausprägungen von Sicherheitskultur 25

5.3 Probanden/-innen und Beziehungspflege 27

5.4 Zwischenfazit 29

6. Wirkungsanalyse der Lernszenarien, ihrer Gestaltung und Usability 31

6.1 Wirkungsanalyse der Lernszenarien 31

6.1.1 Sicher zuhause wohnen & arbeiten 31

6.1.2 Kundendaten sicher managen in Cloud & Co. 31

6.1.3 Die 5 Phasen des CEO Fraud 33

6.1.4 Mobile Kommunikation, Apps & Co. 35

6.1.5 Cyber Pairs 37

6.1.6 Informationsklassifizierung 39

6.1.7 Messenger, sichere Übertragung, Verschlüsselung 41

6.2 Evaluation der Methode, der Usability und des Designs der LS 43

7. Psychologische Grundspannungen, Typologie und Exkurs Reifegrad 47
7.1 Zusammenfassende Besonderheiten der Gruppendiskussionen und Fokusinterviews 47
7.2 Psychologische Grundspannungen bei der Nutzung von Lernszenarien 49
7.3 Exkurs Security Awareness-Reifegrad und -Messungen 51
7.3.1 KnowBe4: Security Culture Maturity 51
7.3.2 SANS Institute: Security Awareness Maturity Model 53
7.3.3 TreeSolution: Capabilty Maturity Model und Security Awareness Radar 53
7.3.4 Prof. Konrad Zerr: SAI – Security Awareness Index 55
7.3.5 Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt 55
7.3.6 Reifegrad auf Basis des known_sense-Layer-Modells 57
7.4 Passung zur psychologischen Konstruktion von Sicherheitskultur und Typologie von Vorgängerstudien 59

8. Fazit und Empfehlungen sowie Top Learnings im Überblick 63
8.1 Fazit und Empfehlungen 63
8.2 Zusammenfassung der Top-Learnings 65

Literatur 67

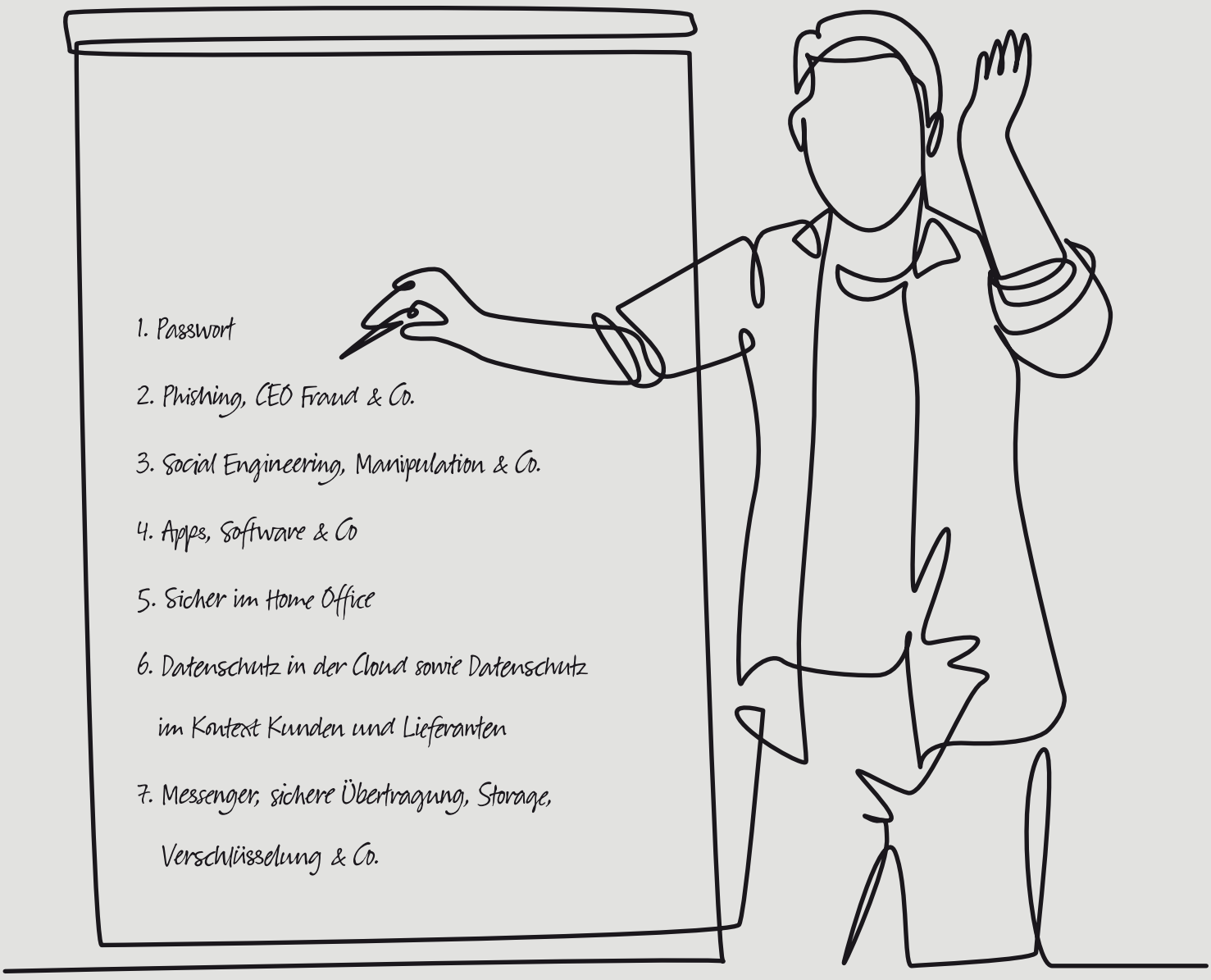


Abb. 1: *Die im Rahmen der KMU-Grundlagenstudie evaluierten Top-Themen für Security Awareness in KMU*

1 Einleitung mit Ausgangslage

Die Technische Hochschule Wildau (TH Wildau) wird im Rahmen des vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderten Projektes „ALARM Informationssicherheit“ gemeinsam mit Partnern bis Ende September 2023 Security Awareness-Werkzeuge entwickeln, die KMU kostenfrei zur Sensibilisierung ihrer Mitarbeitenden zur Verfügung gestellt werden. Geplant sind u. a. sieben analoge Lernszenarien (abgekürzt LS), das heißt gamifizierte Lernstationen, etwa vergleichbar mit der „Security Arena“ von known_sense [1].

Bis zur Feldarbeit waren 6 von 7 LS als Pilotversionen für den Test-Einsatz verfügbar:

- **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“)
- **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** (Thema „Angriffsvektoren bei Wirtschaftsspionage, Cyber Crime, Social Engineering & Co.“)
- **Informationsklassifizierung** (Themen „Klassifizierung“ bzw. „Verwendungszweck von Dokumenten, Daten, Informationen“)

Eine weitere Station befindet sich aktuell in der Entwicklung:

- **Messenger, sichere Übertragung, Verschlüsselung** (Arbeitstitel, geplante Themen: „Messenger“, „sichere Übertragung“, „Verschlüsselung“)

Die in Bezug auf qualitative Security-Forschung erfahrene Kölner Awareness-Agentur known_sense ist im Rahmen des Projektes unter anderem zuständig für den tiefenpsychologischen Teil einer dreiteiligen Evaluationsreihe, deren erster Report-Band, eine tiefenpsychologische Grundlagenstudie zu Security Awareness in KMU, 2021 veröffentlicht wurde [2].

Gleichzeitig evaluiert die TH Wildau die mit dem Projekt verbundenen Fragestellungen per Fragebogen – mithin quantitativ, so dass sich im Rahmen dieser Forschungsaktivitäten die Option hinsichtlich eines Vergleichs („Mapping“) ergibt.

Die im Projekt produzierten Studien werden aus Gründen von Know-how-Transfer und Öffentlichkeitsarbeit publiziert.

Begriffsklärungen mit einem Glossar inklusive grundlegender Definitionen mit vertiefenden Inhalten zu Aspekten wie KMU bzw. KKU, tiefenpsychologische Forschung, Sicherheitskultur, Security Awareness sowie den damit verbundenen Methoden, Grundlagen, Didaktik und Gamification können in der hier angeführten KMU-Grundlagenstudie [2] nachgeschlagen werden.

Weitere Spezifika des Projektes werden in singulären Detailprojekten definiert und sind u. a. über die Projekt-Website [3] abrufbar.

2. Stichprobe und Untersuchungsdesign

2.1 Stichprobe, Test, Moderation, Gruppendiskussionen, Fokusinterviews, Dauer der Befragungen

Es wurden 2 Gruppen mit je 6 Probanden/-innen aus zwei KMU jeweils nach einem 45- bis 60-minütigen Spieletest der LS 45 bis 60 Minuten lang im Rahmen von qualitativen Gruppendiskussionen befragt. Hierfür wurden jeweils drei der bis dato fertigen LS-Prototypen rotierend an- oder durchgespielt.

- Moderiert wurden die LS von einem Kommunikations- und Securityexperten,
- beobachtet wurden sie von einer Diplom-Psychologin mit langjähriger Erfahrung in Bezug auf morphologische Markt- und Medienforschung.
- Anschließend wurden diese zwei Gruppen jeweils einzeln in der jeweiligen „Testbesetzung" von beiden oben genannten Experten/-innen befragt.

Außerdem fanden zwei zusätzliche LS-Tests mit Beobachtung, jedoch ohne anschließende „Gruppendiskussionen" statt.

- Anstelle der Gruppendiskussionen mit den Teilnehmenden wurden anschließend bis zu 45-minütige Fokusinterviews mit den jeweiligen Awareness-Verantwortlichen (den lokalen Veranstaltenden) durchgeführt.
- Aus Gründen der Vergleichbarkeit mit bestehenden LS der „Security Arena" von known_sense [1] wurden hierbei jeweils zwei ältere Security Arena-LS und zwei neue LS aus dem Projekt „ALARM Informationssicherheit" „gegeneinander" (vergleichend) getestet.

2.2 Quotierung der Probanden/-innen

a) Tests mit Befragung innerhalb anschließender Fokusgruppe:

- 1 Gruppe in einem Finanzinstitut für KMU mit Erfahrung in Bezug auf gamifizierte Security Awareness
- 1 Gruppe bei einem produzierenden Familienunternehmen mit Produktionsstätten in Deutschland und Osteuropa – bisher ohne Erfahrung in Bezug auf Security Awareness

b) Zusätzliche Tests ohne anschließende Fokusgruppe, jedoch mit Fokusinterviews der Veranstalter:

- 6 Gruppen mit bis zu 6 Teilnehmenden bei einem Tochterunternehmen eines Versorgers
- 7 Gruppen mit bis zu 11 Teilnehmenden bei einem Unternehmen der Touristikbranche

Die dort getesteten LS wurden jeweils von Security-Kolleginnen bzw. -Kollegen der veranstaltenden Unternehmen moderiert, die von known_sense vor den Trainings-Events bis zu 90 Minuten in Videokonferenzen und zusätzlich ca. 30 bis 45 Minuten am Veranstaltungsort vor Beginn des Events gebrieft bzw. während und zwischen der Moderation supervidiert wurden.

Stichprobe a) und b): insgesamt 120 Probanden/-innen.

Rollen: Die o. g. Stichprobe berücksichtigte Management, Führungskräfte und andere Mitarbeitende aller Geschlechter (w, m, d).

Alter: Die Gruppen setzten sich in etwa zu gleichen Teilen aus den Altersgruppen 18–25, 26–35, 36–45, 46–55, > 55 Jahre zusammen.

Sprache: Bei allen Organisationen wurde in deutscher Sprache getestet. Jedoch wurden 4 Gruppen aus b) mit internationalen Teilnehmenden aus ca. 10 verschiedenen Ländern in englischer Sprache moderiert. Zwei Pilotstationen (CEO Fraud, Sicher zuhause wohnen & arbeiten) wurden hierfür kurzfristig übersetzt.

Besonderheiten bezüglich Corona: Zu sämtlichen Tests und Befragungen wurden von allen Beteiligten die Masken abgelegt.

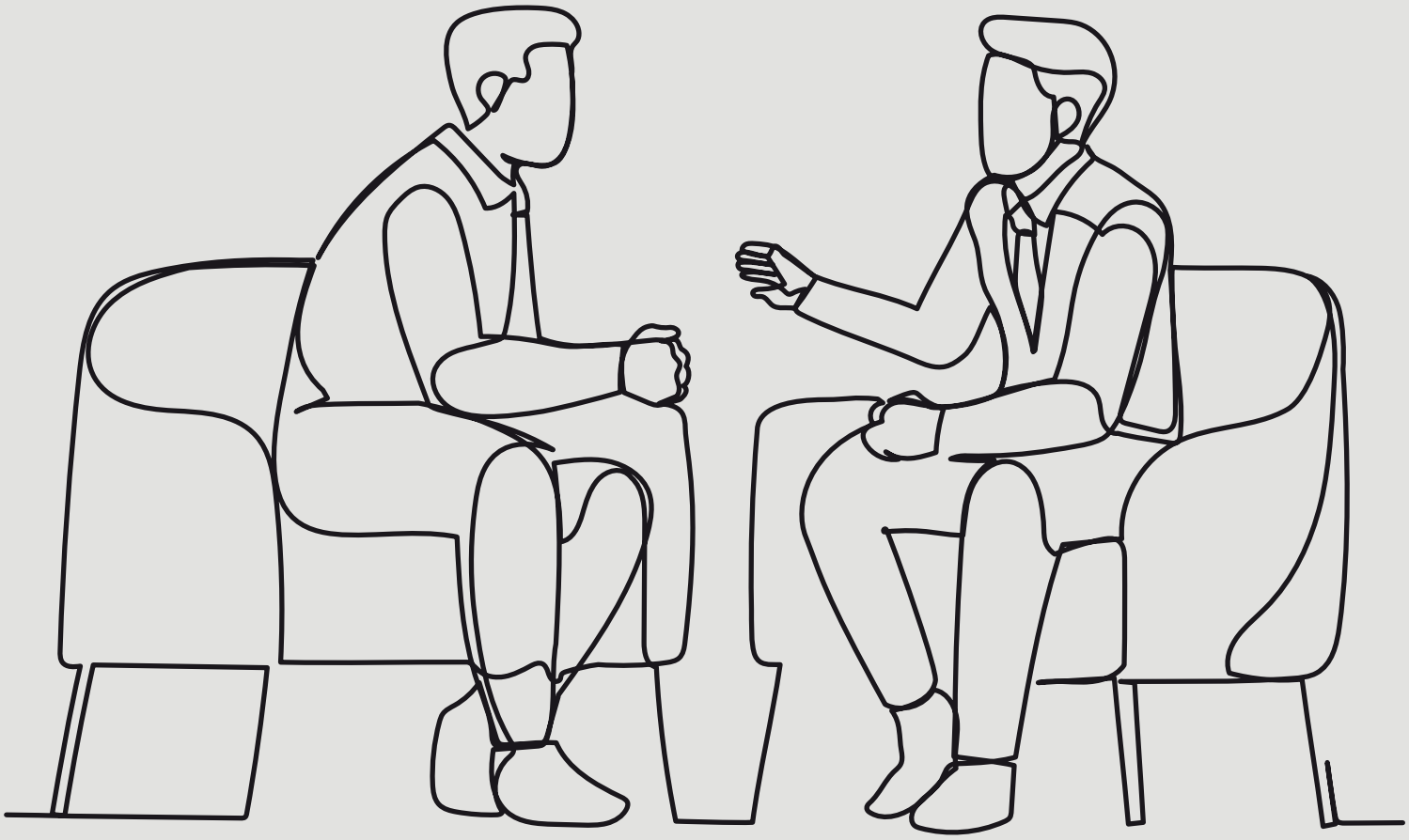
Alle Befragten wurden hinsichtlich der Teilnahme für 60 bis 120 Minuten von ihrer Arbeit freigestellt und nutzen sowohl im beruflichen wie auch im privaten Kontext digitale Kommunikationstechnologien. D. h. alle befragten Personen

- arbeiten beruflich an einem PC mit Internetanschluss,
- telefonieren in ihrem beruflichen Kontext täglich,
- verfügen zu Hause über einen Internetanschluss und nutzen diesen täglich,
- verfügen über ein internetfähiges Smartphone und nutzen dieses täglich,
- sind regelmäßig in sozialen Netzwerken, Communities, Internetforen, Blogs oder im Firmenintranet bzw. Wiki o. ä (Mehrfachnutzung möglich) aktiv.

Untersuchungsorte: Nordrhein-Westfalen und Hessen. Die Tests bzw. Befragungen fanden bei drei Organisationen in Gebäuden der Unternehmen statt, die geeignete Räume mit Tischen für den Test der LS zur Verfügung stellten. Bei einem vierten Unternehmen wurde eine sehr exponierte, imageträchtige Event-Location außerhalb der Organisation angemietet.

Unternehmensgröße: Mittlere Unternehmen (120 bis 240 Mitarbeitende)

Zeitraum Feldarbeit: Juni bis Juli 2022



Analysezeitraum: Juli bis August 2022

Zeitraum Studienerstellung: Juli bis September 2022

Projektteam: Diplom-Psychologinnen und -Psychologen bzw. qualitative Marktforscherinnen und-forscher sowie Kommunikationsexpertinnen und -experten mit Projektleitung durch Diplom-Psychologin Ankha Haucke und Dietmar Pokoyski

Produktion: known_sense im Auftrag der TH Wildau

Ansprechpartner: Dietmar Pokoyski,
sense@known-sense.de, Telefon +49 2203 1831618

1	**Support-Betrug (Microsoft Scam)** Angebliche Mitarbeitende eines Technologie-Anbieters (z. B. Microsoft) versuchen via Internet oder Telefon Zugriff auf meinen PC zu erlangen. Dabei können u. a. auch gefälschte Warnhinweise am Rechner zum Einsatz kommen.	**A** Achten Sie auf gefälschte Warnungen am PC und auf Anrufe von potenziellen Supportern bekannter Technologie-Unternehmen, die versuchen, Ihnen einzureden, Ihr PC sei von Malware befallen. Beenden Sie sofort das Gespräch. Haben Sie sich bereits mit einem Betrüger oder einer Betrügerin eingelassen, trennen Sie Ihren PC vom Netz und ändern Sie Ihre Passwörter.
2	**Ungesperrte Rechner** Können dazu führen, dass eine nicht autorisierte Person (z. B. Einbrecher, Reinigungskräfte, Haushaltshilfen, Haushaltsangehörige, Besucher) Zugriff auf meinen PC bzw. meine digitale Identität erhält und diese missbräuchlich oder versehentlich nutzt.	**C** Auch für das Homeoffice gilt das Clear-Desk-Prinzip: Bildschirm sperren (Win + L), wenn Sie den Arbeitsplatz verlassen.
3	**Passwörter** Auf Zetteln oder in anderen Dokumenten notiert, können nicht autorisierte Personen darauf zugreifen und meine Identität missbrauchen.	**B** Passwörter niemals aufschreiben – auch nicht im Homeoffice. Passwortmanager nutzen. Darüber hinaus sämtliche interne bzw. (streng) vertraulichen Papierdokumente sicher verschließen.

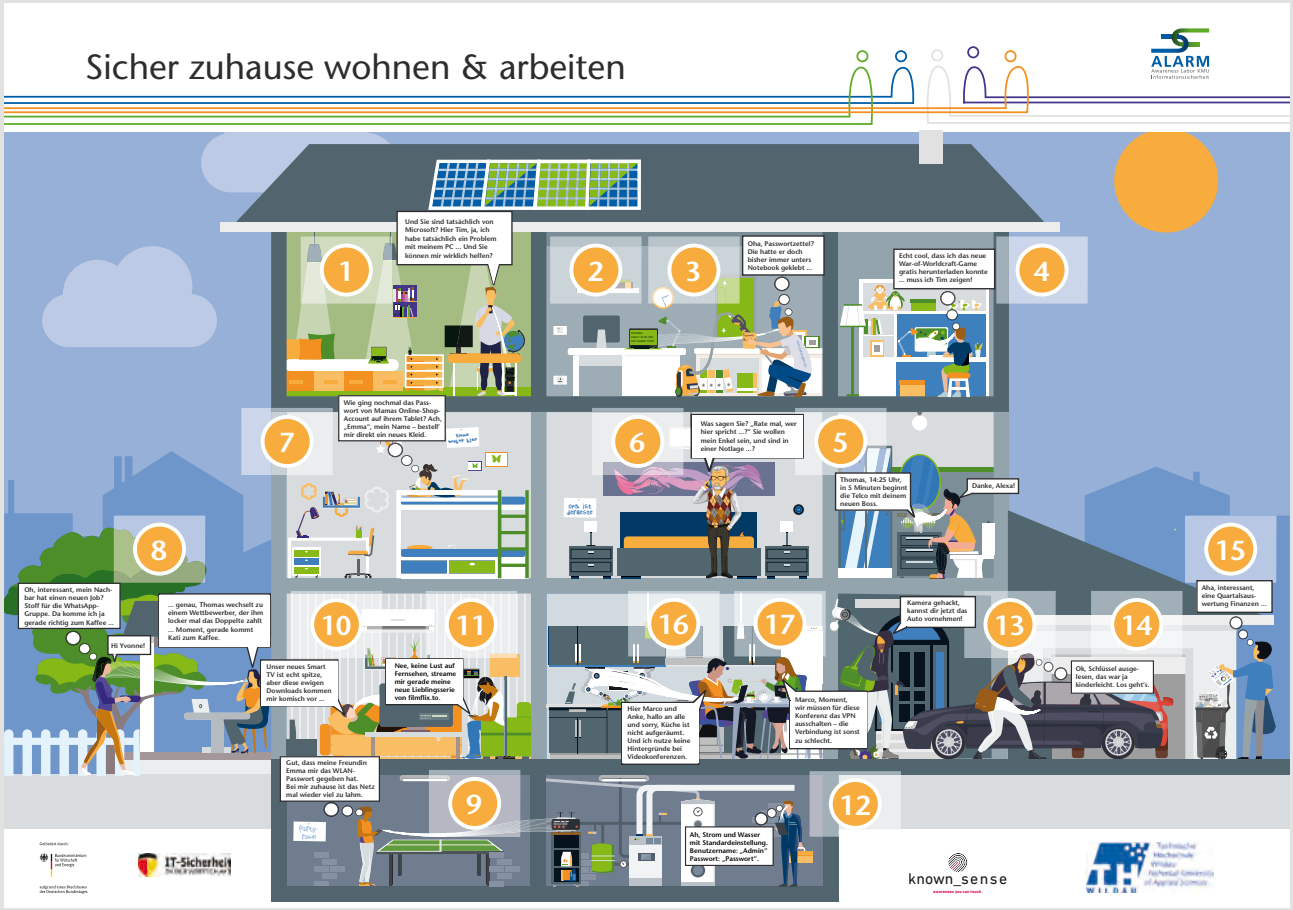


Abb. 2 und 3: *LS „Sicher zuhause wohnen & arbeiten“: Auszug Lösungsblatt (oben), Spielfeld (unten)*

3 Lernszenarien-Methodik bzw. Übersicht Lernszenarien-Testmaterial

3.1 Lernszenarien-Methodik

Bei einem typischen LS-Training durchlaufen Teams synchron verschiedene Themenstationen, an denen sie von Moderrierenden hinsichtlich verschiedener Sicherheits-Themen sensibilisiert werden. Bei der synchronen Verzahnung von LS 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"* [4].

„Eine Lernstation 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 Lernstation 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." [5]

Lernstationen bieten diverse Vorteile gegenüber herkömmlichen Schulungsformaten:

1. Nutzung als Teaser, *„um weitere Wissensbedarfe bei den Teilnehmenden zu sicherheitsrelevanten Fragen zu erzeugen und somit innerhalb einer Sicherheitskommunikationskampagne als entscheidender Baustein zu dienen"* [5].
2. 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.
3. Leichte Adaption an die Bedürfnisse der anwendenden Organisation mit bedarfsweiser Weiterentwicklung.
4. 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 Teambuilding"* [5]. Außerdem sprechen die Teilnehmenden nach *„Absolvierung der Lernstationen über die dort erlebten Themen sowie das Format selbst"* [5].
5. Lernstationen können potenziell *„auch bei Organisationen mit unterentwickeltem Reifegrad zum Schulungs-Thema angewendet werden"* [5].

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 á 15 Minuten (gesamt demnach eine Stunde), die synchron gegenüber teilnehmenden Teams mit bis zu je 12 Personen von eigenen Mitarbeitenden moderiert werden. Auf diese Weise können in 60 Minuten bis zu 48 Teilnehmende per LS sensibilisiert werden. Bei bis zu fünf Wiederholungen sind dies 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 Teilnehmenden je 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"* [5].

Die Moderation läuft in drei Stufen ab:

1. LS-Briefing mit Vorstellung von Moderation und Thema, Abfragen von Erfahrungen in Bezug auf das jeweilige LS-Thema mit Team-Diskussion
2. LS-Spiel (Simulation, im Rahmen der „Security Arena" in der Regel „Minigame" genannt)
3. 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 Moderationsleitfaden 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 das Gelingen der Lernstation 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

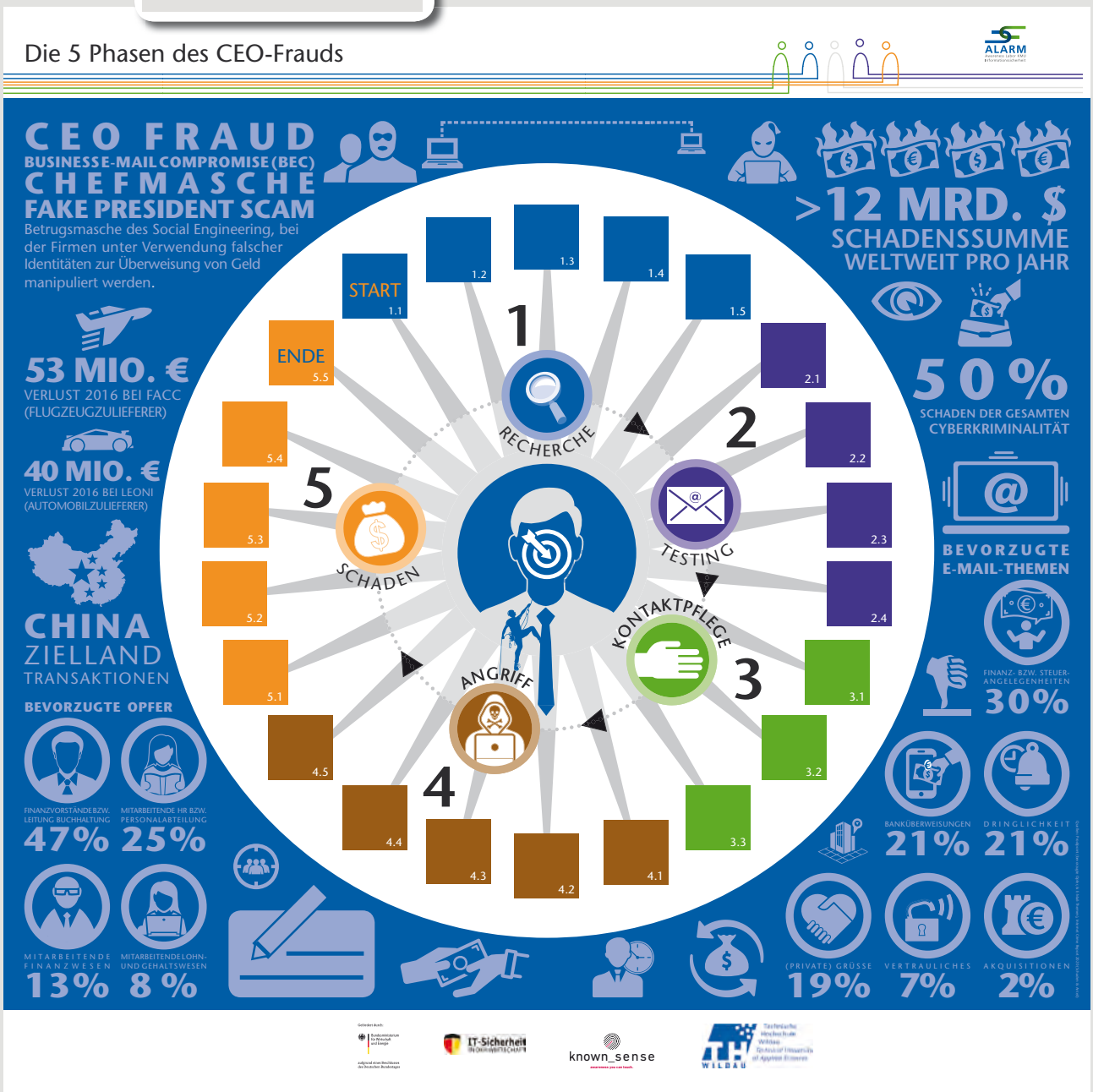


Abb. 4: *LS „Kundendaten sicher managen in Cloud & Co.“: Auszug Spielkarten (oben)*
Abb. 5: *LS „Die 5 Phasen des CEO Fraud“: Spielfeld (unten)*

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.“ [5]

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.“* [5]

Sämtliche LS 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 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.“ [1]

LS bilden in ihrer Ausschließlichkeit kein probates Medium hinsichtlich einer dauerhaft wirksamen Security Awareness. Eine nachhaltige Kampagne kann nur im Mix mit weiteren Medien und Kanälen und bei ausreichender Zielgruppendiversifikation unter Berücksichtigung geeigneter psychologischer Verfassungen erfolgen. LS sind jedoch aufgrund der Kürze und hohen Sichtbarkeit innerhalb der Organisation ein idealer Teaser für einen Kampagnen-Kickoff – auch weil hierüber unter den Teilnehmenden potenziell Bedarfe für weitere Maßnahmen geschaffen werden. D. h. die bzw. der ideale Mitarbeitende ist sich nach dem Durchlaufen der LS durchaus bewusst, dass sie bzw. er nicht vertiefend sensibilisiert wurde, sie bzw. er bildet jedoch bestenfalls für sich Fragen, deren Beantwortung den Bedarf nach weiteren Awareness-Maßnahmen erzeugen. Darüber werden im Sinne einer integrierten Kommunikation auch weitere Maßnahmen implizit beworben.

3.2 Übersicht Lernszenarien-Testmaterial

Die Themen der entwickelten und hier getesteten LS-Prototypen ergeben sich aus den Ergebnissen bzw. einem Ranking der KMU-Grundlagenstudie. [2]

3.2.1 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 (9 Seiten)

Im Rahmen dieses LS 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

3.2.2 Kundendaten sicher managen in Cloud & Co.

Das Spiel besteht aus:

- 1 Spielfeld (100 x 70 cm), das im Zentrum 20 nummerierte Sortierfelder abbildet
- 20 Spielkarten (DIN A6) als Klappkarten (U1-U4):
  - vorne (U1) 20 verschiedene Passwortphrasen
  - hinten (U4) auf den 10 Karten mit den „stärksten“ Passwortphrasen Aussagen zum Thema Kundendatenschutz im Stil von „Goldenen Regeln“ – davon 7 zutreffende (richtige) und 3 falsche; auf den 10 Karten mit den „schwächsten“ Passwortphrasen Hinweise, warum diese als „schwach“ zu betrachten sind und Tipps für eine Optimierung
  - Innen (U2/U3) auf den 10 Karten mit den „stärksten“ Passwortphrasen 10 Aussagen zum Thema sichere Cloud – davon 5 zutreffende (richtige) und 5 falsche
- Moderationsblätter mit Lösung (10 Seiten)

Abhören und Mitschnitte anfertigen
Weitgehend unbemerkter Zugriff auf Hardware-Steuerelemente meines Geräts (z. B. Kamera, Mikrofon), um unberechtigt Bild- bzw. Ton-Mitschnitte durchführen und diese verwerten zu können.

Surfverhalten bzw. Nutzerdaten auslesen
Zugriff auf personenbezogene Daten und Nutzerdaten (z. B. Kontakte, Fotos, Kalendereinträge), um diese auszulesen, zu verändern, zu löschen oder an Werbepartner weiterzuleiten.

A

Wenn Zugriff auf Kamera bzw. Mikrofon von einer App nicht benötigt wird, ermögliche ich dieser nicht, Fotos oder Mitschnitte mithilfe meiner Hardware anzufertigen. Ich überprüfe die Berechtigungen der App und deaktiviere diese notfalls.

C

Ich versuche, so wenig personenbezogene Daten wie möglich zu erzeugen, indem ich Zugriffsrechte bei Apps und damit das Nutzer-Tracking auf das Nötigste beschränke. Somit hinterlasse ich beim Surfen, aber auch in Social Media, so wenig Spuren wie möglich.

Geolocation
Zugriff auf meinen Standort – ungefähr (netzwerkbasiert) oder genau (GPS). Damit können Bewegungsprofile von mir erstellt werden, die Anbieter dabei unterstützen, mir möglicherweise unerwünschte Werbung zu senden.

E

Ich installiere ausschließlich Apps, die ich tatsächlich benötige und vergebe nur Berechtigungen, die diese Apps zur Ausführung benötigen. Apps, die ich nicht mehr nutze, deinstalliere ich. Mobiles Internet, WLAN, Bluetooth und GPS schalte ich bei Nichtgebrauch ab.

Abb. 6 und 7: *LS „Mobile Kommunikation, Apps & Co.“: Auszug Spielkarten (oben), Spielfeld (unten)*

Im ersten Teil sollen die 20 Karten mit den Passwörtern (violett) entsprechend der jeweiligen Stärke gerankt werden, indem sie auf den 20 Feldern des Spielfeldes in der richtigen Reihenfolge von „stark“ bis „schwach“ verteilt werden. **Im zweiten Teil** werden die 10 als schwächste Passwörter gerankten Karten (Rang 11–20, d. h. die unteren beiden Reihen) umgedreht und die 10 stärksten Passwörter (Rang 1–10, d.h. die beiden oberen Reihen) ebenfalls. Oben sollen die blauen Rückseiten liegen, unten die orangen. Die unteren Reihen werden aus dem Spiel genommen. In den beiden oberen Reihen sollten idealerweise ausschließlich violette Karten liegen mit Aussagen zum Thema Kundendatenschutz. Hieraus sollen im zweiten Teil 3 falsche Aussagen aussortiert und vom Spielfeld gezogen werden, so dass 7 richtige Aussagen übrigbleiben. Ist unter den bei den Top 10 gerankten Karten eine falsche (orange), wird diese aus dem Spiel genommen und mit den verbliebenen Karten weitergespielt. **Im dritten Teil** sollen die übrig gebliebenen Karten (insgesamt 7) geöffnet und auf das geschlossene Format umgeschlagen werden, so dass die U3 oben liegt und lesbar ist. Hierauf befinden sich, wenn die Karten bisher richtig sortiert wurden, Aussagen zum Thema Cloud. Die richtigen Aussagen sollen dem jeweils passenden Icon auf den ersten vier Feldern in der ersten Reihe zugeordnet werden. Maximal vier Aussagen sind richtig, d. h., wenn vorher keine Fehler passiert sind. Befindet sich im Innenteil eine weiße, unbedruckte Fläche, weist dies auf einen Fehler in der ersten Runde hin; bei Fehlern der zweiten Runde erscheint im Innenteil ein entsprechender Hinweis; die Karten werden dann aus dem Spiel genommen.

Didaktische Intention: Starke Passwörter bilden und verwenden sowie sicherer Umgang mit Kundendaten – vor allem in der Cloud

Geplante Nettospielzeit: 3 x 2 Minuten (gesamt 6 Minuten)

Maximale Punktzahl: 55

Potenzielle Zielgruppe: alle, insbesondere hinsichtlich Teil 2 und 3 Projektmanagement, Kundenservice bzw. Kundenmanagement, Vertrieb u. a. Mitarbeitende mit intensivem Kundenkontakt

3.2.3 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 (12 Seiten)

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: Mitarbeitende der Finanzbuchhaltung, des Controllings und der HR-Abteilung, Management und andere Führungskräfte

3.2.4 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 (9 Seiten)

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 LS 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)

E

Betrugsmasche, bei der sich Cyber Kriminelle u. a. als Chef ausgeben, um unberechtigt Geld auf ihre Konten transferieren zu lassen.

3

CEO

19

FRAUD

k

Ich überprüfe potenzielle Vorgesetzte, die anrufen oder schreiben, stets in Bezug auf ihre Identität und Motive.

A

Form sozialer Manipulation zur Informationsgewinnung.

1

SOCIAL

17

ENGINEERING

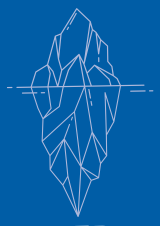
i

Ich stelle die Identität bzw. Berechtigungen von Gesprächspartnern sicher – immer.

D

Äußerst echt aussehende, manipulierte Medieninhalte.

26



DEEP...

15

FAKE

g

Nichts ist so wie es scheint – bei verdächtigen Bildern, Videos oder Tonaufnahmen achte ich auf auffällige „Fehler".

F

Lösegelderpressung mithilfe von Malware, die die Täter in IT-Systeme schleusen, um den Zugriff auf Daten bzw. Systeme zu unterbinden.

27

RANSOM...

14

WARE

f

Ich untersuche E-Mails stets kritisch auf Phishing und öffene niemals unbekannte Anlagen bzw. Links.

J

Social-Engineering-Methode mithilfe präparierter Wechseldatenträger.

29

USB

12

DROPPING

d

„Fremde", d. h. nicht verifizierte Datenträger, werden von mir nicht genutzt.

Abb. 8: *LS „Cyber Pairs": Auszug Spielkarten*

Maximale Punktzahl bei Incentivierung: 24

Potenzielle Zielgruppe: alle

3.2.5 Cyber Pairs

Das Spiel besteht aus:

- 32 blaue Cyber-Memokarten (7x7 cm, Ziffern-Codes: #1-32, einseitig)
- 16 orange Cyber-Risikokarten (7x7 cm, Großbuchstaben-Codes: #A-P, beidseitig)
- 16 grüne Cyber-Schutzkarten (7x7 cm, Kleinbuchstaben-Codes: #a-p, beidseitig)
- Moderationsblätter mit Lösung (8 Seiten)

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 abgelegt werden. **In einem dritten Durchgang** sollen die 16 grünen Cyber-Schutzkarten passend neben den orangenen 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

3.2.6 Informationsklassifizierung

Das Spiel besteht aus:

- 50 Holzklötzchen, 15 cm lang (bedruckt mit Beschreibungen diverser typischer Dokumentenarten)
- 15 verschiedenfarbige Verwendungszweckkarten in 5 Kategorien, 3 für jede Kategorie (A-E, Farben: orange, grün, blau, violett, braun)
- Geplant, jedoch nicht getestet: Ein Spielfeld zum Bauen von Holztürmen bzw. als Container für die Verwendungszweckkarten
- Moderationsblätter mit Lösung (9 Seiten)

Es werden **im ersten Teil** aus maximal 50 Holzklötzchen mit den Aufdrucken typischer Dokumenten- bzw. Informationsarten analog der in den meisten Organisationen verwendeten vier Klassen einer Klassifikation vier Holztürme gebaut. **In einem zweiten Teil** sollen in die Türme 15 Verwendungszweckkarten analog einer sicheren Verwendung (Weitergabe, Vernichtung etc.) eingeworfen werden.

Didaktische Intention: Schutzbedarf von Informationen kennen und entsprechend des jeweiligen Risikos klassifizieren können, Verwendungszwecke differenziert betrachten

Geplante Nettospielzeit: 4 + 2 Minuten (gesamt 6 Minuten)

Maximale Punktzahl: 65

Potenzielle Zielgruppe: alle, die mit sensitiven Informationen umgehen

3.2.7 Messenger, sichere Übertragung, Verschlüsselung

Diese LS wurde nicht getestet, da zum Zeitpunkt der Feldarbeit nur ein Grobkonzept vorlag. Allerdings wurde das Grobkonzept, das in Bezug auf das Spiel zwei Teile beinhaltet, den Awareness-Verantwortlichen im Rahmen von Fokusinterviews kurz vorgestellt und um eine erste Reaktion gebeten. **In Teil 1** sollen verschiedenen Messengern, dargestellt durch ihre Logos, Risiken zugeordnet werden. **Teil 2** umfasst eine Verschlüsselungsaufgabe.

3.2.8 Zusammenfassung Kapitel 3

In der Tabelle auf der nächsten Seite werden die für die in den LS verwendeten Spiele typischen Spielprinzipien – bei den LS des hiesigen Projektes sind es 4 von 6 stets wiederkehrenden Prinzipien (siehe Kolarows Masterthesis [5], S. 52) – als Übersicht dargestellt:

- richtig vs. falsch
- 1:n- oder Prozess-Zuordnung
- Zuordnen & Handeln (Wimmelbildlogik)
- Schätzung und/oder Ranking

Kapitel	3.2.1	3.2.2	3.2.3	3.3.4	3.2.5	3.2.6
LS **Spielprinzip**	Sicher zu-hause wohnen & arbeiten	Kundenda-ten sicher managen in Cloud & Co.	Die 5 Pha-sen des CEO Fraud	Mobile Kom-munikation, Apps & Co.	Cyber Pairs	Informa-tionsklas-sifizierung
richtig vs. falsch		X	X			
1:n- oder Prozess-Zuordnung	X		X	X	X	X
Zuordnen & Handeln (Wimmel-bildlogik)	X			X		
Schätzung und/oder Ranking		X	X			

Abb. 9: *Typische Spielprinzipien der LS im Überblick*

4. Erste Eindrücke aus der Akquise bzw. Feldarbeit

Die Akquise von Unternehmen hinsichtlich einer Teilnahme an dieser Wirkungsanalyse erweist sich als extrem schwierig und langwierig.

Zahlreiche angefragte Institute der Markt- und Medienforschung, zu deren Services die Probanden/-innen-Akquise im Sinne einer passenden Quotierung gehört und die von den Produzierenden dieser Studie in den letzten 20 Jahren regelmäßig in Anspruch genommen wurden, lehnen bei Anfrage adhoc ab, bei diesem Forschungsvorhaben zu unterstützen. Selbst eine Reduktion der Ansprüche der Produzierenden dieser Wirkungsanalyse führt nicht zu dem erwünschten Ergebnis, wie u. a. folgende Zitate belegen:

„Hochschulen sind schwierige ‚Partner' – machen wir nicht mehr und in der angefragten Form können wir das eh nicht realisieren."

„Erst Corona und jetzt kommen Sie noch mit so einem komplexen KMU-Projekt (…). Für Sie haben wir bisher alles gemacht, aber nein, dafür haben wir gerade wirklich nicht die Ressourcen."

„Eine derartige Quotierung zu erfüllen ist beinahe unmöglich – geht einfach nicht, für kein Geld der Welt! Sorry."

Die reflexartige Idee, die Partnerunternehmen aus dem Projekt „ALARM Informationssicherheit" als Testumgebung einzubeziehen, wird schnell verworfen, weil aus Sicht der Herausgebenden hierbei nicht ausreichend Anonymität gewährleistet wäre und die bereits bestehende Bindung zu den Partnerunternehmen mit den zur Verfügung gestellten Informationen auf die hiesige Befragung abfärben würde. Daher müssen die an diesem Test teilnehmenden Organisationen schließlich von den Produzierenden dieser Studie persönlich akquiriert werden.

Bei der Akquise werden Anfragen zur Teilnahme direkt über known_sense gestellt. Einige wenige Unternehmen scheinen sich vor Begeisterung ob einer Teilnahme an einem Awareness-Werkzeug-Test zu überschlagen, da sie offensichtlich Sensibilisierungsmaßnahmen planen und sich einen Motivationsschub erhoffen.

Bei anderen kommt es zu einem langwierigen Hin und Her mit mannigfaltigen Zu- und anschließenden Absagen. Dabei ist stets die Ambivalenz spürbar mit der Frage, ob dem eigenen Aufwand mit der kostenfreien Abstellung von Personal und dem mit ihnen verbundenen Arbeitszeitverlust auch ein konkreter Nutzen gegenüber stehen, und ob in Zeiten von Corona Präsenztrainings nicht ein zu großes Risiko darstellen würden. Folgende Zitate stehen dafür:

„Eigentlich rät man uns davon ab, aber wir sind es leid, ausschließlich digital zu kommunizieren."

„Wir wollen genau sowas – auch wenn die Geschäftsleitung das gerade nicht gern' sieht."

Die Organisationen, die zu einer Teilnahme überzeugt werden können, stammen ausschließlich aus dem Kontext „mittlere Unternehmen." Kleine Unternehmen oder Kleinstunternehmen, die von uns kontaktiert werden, geben ohne Ausnahme an, keinen Bedarf in Bezug auf Sensibilisierung zu haben. In den Telefonaten wird aber auch Überforderung deutlich, sich überhaupt mit dem Thema Awareness auseinanderzusetzen:

„Tut mir leid, bei uns ist praktisch alles verboten, das brauchen wir nicht."

„Bei uns gibt's Ansprachen vom Chef – die sind dann zu befolgen, sonst knallt's."

„Wie kommen sie nur auf uns? Wir haben 14 Mitarbeiter, das lohnt sich doch gar nicht."

Insbesondere während der Verhandlungen mit den jeweiligen Kontaktpersonen, die in der Regel auch die Awareness-Verantwortlichen in ihren Organisationen stellen, wird gewahr, dass diese bereits bei Anfrage und Planung gedanklich mögliche Zielgruppen bilden, denen sie über den Test eine kostenfreie Awareness-Veranstaltung verschaffen wollen – wie etwa folgende Zitate belegen:

„Prima, ich weiß schon genau, wen ich da schicke."

„Wir haben da so ein paar Spezis – die habe ich im Blick, denen würde das mal gut tun."

„Und das kostet uns wirklich keinen Cent?"

In vielen Fällen müssen interne Akquisitionsüberlegungen durch die Awareness-Verantwortlichen in Richtung „ausschließlich Management" von uns unterbrochen werden, um die intendierte Quotierung zu halten:

„CEO Fraud (?) – das ist ja super, da schicke ich Ihnen direkt unser komplettes Management und die Buchhaltung noch dazu – dann sollen die sich das mal schön anhören.“

Die ursprünglich für April bis Mai 2022 terminierten Tests müssen schließlich aufgrund von Corona-Infektionen quer durch alle Beteiligten auf Juni bzw. Juli 2022 verschoben werden. Dabei können sämtliche Termine ohne Verluste bzw. Ersatz-Organisationen verlegt werden.

Obwohl die befragten Organisationen sich in Bezug auf Größe bzw. Anzahl von Mitarbeitenden wenig unterscheiden, werden deutliche Unterschiede in Bezug auf Auftritt bzw. Unternehmenskultur gewahr, die sich unter anderem auch anhand der hier und in Kapitel 5 ausgewählten Zitate verdeutlichen lassen.


Erste Hilfe
Erste Hilfe
Werkstatt
U-BAHN

5. Atmosphärisches im Kontext Unternehmens- bzw. Sicherheitskultur und Kommunikation in den KMU

5.1 Generelles bzw. Ausprägungen von Unternehmenskultur

Räumlichkeiten …

- … von stillen, ausladenden, dunklen, bis auf ein geräuscharmes Großraumbüro menschenleeren Räumen ohne jede auffällige, persönliche Interieur-Note und ohne Rezeption, Wartebereich bzw. Anzeichen von Besucherreglungen, Betrieb oder Geschäftigkeit bis hin zu luftig, freundlich mit Rezeption, klaren Reglungen, bequemen Sitzplatzangeboten im Wartebereich, schickem Einrichtungs-Understatement mit ausgewählter Kunst oder umgebender Dachbegrünung,
- … von der Mitbenutzung gemeinschaftlicher Coworkingspaces bis hin zur bewussten Anmietung einer exklusiven Event-Location außerhalb des Firmenstammsitzes für den Test.

Testräume …

- … von pragmatisch-praktisch, d. h. ungemütlich, kühl und eng, bis großzügig bzw. weitläufig und luftig.

Bewirtung von Gästen …

- … von der gut ausgestatteten Gemeinschaftsküche mit Herd, Mikrowelle, diversen Getränke-Kühlschränken und Speiseeis-Truhe mit Selbstbedienung …

„Lutschfinger oder Magnum (?) – bedient euch einfach …“

- … über das klassische Plätzchen-Gedeck mit Kaffee bis hin zu Platzdeckchen mit jeweils individuellen Kaffeekännchen und dekorierten Puddinggläschen bzw. expliziter Einladung, gemeinsam mit den Probanden/-innen nach dem Test ein Mittagessen einzunehmen.

„Bei derartigen Veranstaltungen essen wir als Team stets gemeinsam; Sie sind herzlich dazu eingeladen..“

5. 2 Ausprägungen von Sicherheitskultur

Auch in punkto Sicherheitskultur werden deutliche Unterschiede spürbar, im weiteren Verlauf von entsprechenden Zitaten unterfüttert.

Eintreffen bzw. Begrüßung …

- … von sicheren Prozessen in Bezug auf Zugangskontrolle mit Eingangs- bzw. Wartezonen, Anmeldung und expliziter Abholung bis hin zu offenem Reinspazieren in zum Teil als kritisch wahrgenommene Unternehmensbereiche.

Corona-Maßnahmen …

- … von eher läppsch …

„Maske? So wie man mag …“

- … bis hin zu sorgevoll geäußerten Bedenken, Masken abzulegen und einem weitläufigen Testraum mit großen Abständen an überdimensionierten Vorstands-Konferenztischen, Hochtechnik suggerierenden Belüftungsgeräten, großen offenen Fenstern und CO^2-Meldern.

Homeoffice …

- … von nahezu 100% während des pandemischen Hochs, z. T. auch an ausländischen Wohnorten der Mitarbeitenden, bis hin zur Nulllösung.

„Homeoffice, nee, wir mussten hier antreten – alle.“

In einem als besonders entspannt empfundenem Unternehmen erzählt man, wie man den Homeoffice-Prozess im Zuge der Pandemie erlebt hat.

„Homeoffice (?) – mit Leichtigkeit …“

„Das war eine schnelle und reibungslose Umstellung. Ich hab jetzt nur zum Telefonieren eine App auf dem Handy.“

Digitalisierung bzw. (Online-)Zugänge. …

- … für die Mitarbeitenden von restriktiv, d. h. für wenige mit umfangreichen Rechten und ausschließlich expliziten Bereichsstationen mit selektivem Online-Zugang für den Rest, bis hin zur Förderung bei der Nutzung innovativer Tools bzw. Apps mit dem Wunsch *„noch agiler aufgestellt zu sein.“*

„Technik? Sehr viel! Wir sind hier wahrlich in einer Luxus-Situation.“

„Spielen ist auch eine schöne Möglichkeit, Technologie und ihre Risiken erfahrbar zu machen.“

„Fehler passieren überall. Wir machen hier auch ‚Learning by doing.“

oder

„Wir haben hier zwei, drei Internet-Rechner und einen einzigen exklusiv mit Kundendaten für insgesamt drei Firmen, unter denen wir auftreten."

„Alles komplett auf ‚digital' umzustellen (?) – zu zeitintensiv."

„Wir sind wie ein gallisches Dorf. Als ich hier anfing, habe ich gedacht, ich bin im 18. Jahrhundert."

Sicherheits-Organisation, Fehlerkultur und erlebte Vorfälle …

- … von der Übertragung sämtlicher Aufgaben an einen IT-Administrator bzw. eine IT-Administratorin bis hin zum mehrköpfigen Security-Team.

„Das Thema Sicherheit ist hier sehr konkret."

oder

„Sicherheit ist wichtig, klar, aber die Themenvielfalt überfordert die meisten von uns."

In einem Unternehmen erscheint die Präsenz und Stellung der externen Datenschutzbeauftragten deutlich wichtiger als die des intern agierenden und für Informationssicherheit zuständigen IT-Administrators.

In diesem Unternehmen werden darüber hinaus bereits zu Beginn des Tests Reaktionen auf Fehler entlang von Schuld und Scham sehr offensiv angesprochen.

„Wir können ja nicht alles wissen, wenn was passiert, muss man offen darüber reden können, auch wenn das vielleicht manchmal nervt."

Vorfälle sind bei allen Organisationen an der Tagesordnung, insbesondere CEO Fraud und Telefonbetrug. Es gibt kein Unternehmen, das nicht bereits von CEO Fraud betroffen war.

„Wir sind hier fast schon ‚per Du' mit den angeblichen Interpol-Kommissaren, die hier ständig anrufen."

Zum Stichwort „Phishing" wird in einem Unternehmen von zwei konkreten Vorfällen erzählt, durch die man *„kurz vor der Katastrophe"* gewesen sei. Dabei habe man gemerkt, dass man *„nicht alles mit Technik lösen"* könne. Die hiesige Sicherheitskultur wird als offen und kommunikativ erlebt.

„Die Leute fragen oft nach, lieber einmal mehr als weniger, vor allem bezüglich E-Mails. Da bin ich echt stolz auf unsere Leute." (IT-Mitarbeiterin)

Awareness-Erfahrungen …

- … von …

„… so gut wie gar nicht, außer ab und an Gespräche mit dem IT-Admin …"

- … bis hin zu regelmäßigen Schulungen.

Bei einer Organisation wurde bereits vor einigen Jahren LS der „Security Arena" lizenziert.

„Wir konnten diese jedoch wegen der Corona-Pandemie noch nicht in dem Maße einsetzen, wie wir es ursprünglich geplant hatten."

Bei einer weiteren Organisation wurde bereits zwei Jahre zuvor eine „Security Arena" als Eintages-Event erfolgreich durchgeführt.

„Das war schon motivierend für alle, aber für weitere Maßnahmen reichte die Zeit leider nicht."

In dem als besonders entspannt empfundenen Unternehmen wird dem Thema innerhalb eines monatlichen Jour Fixes Raum gegeben. Hier werden z. B. Youtube-Videos mit „Awareness-Inhalten" gezeigt und besprochen und es wird ein vom IT-Leiter ausgewählter „Security Fall des Monats" diskutiert.

„Wir erschlagen viel mit Technik, aber es gibt auch häufig kleine, praxisnahe Häppchen,"

… lautet die Devise.

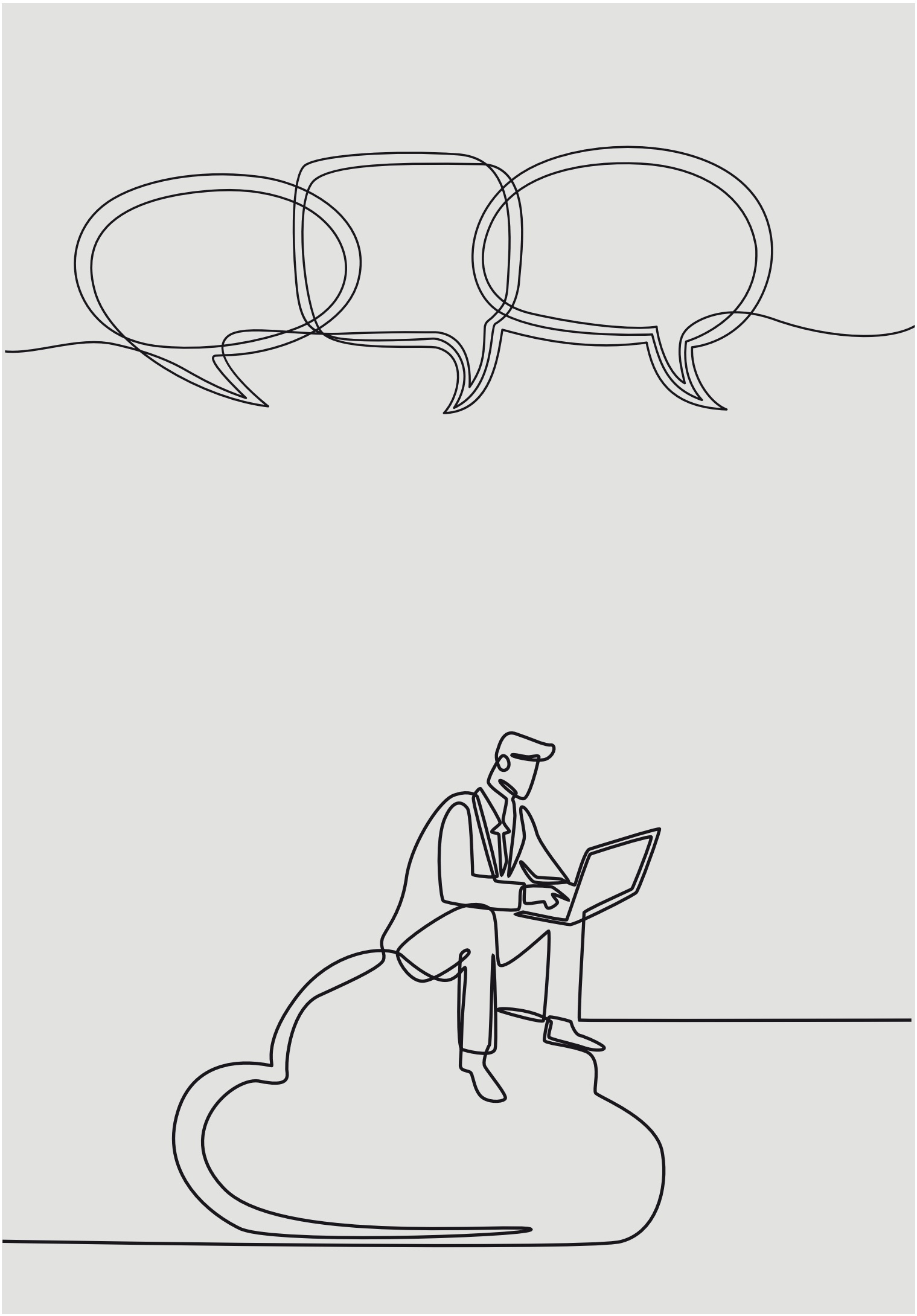
„Awareness ist hoch gehängt und es gibt einen guten Draht zur IT. Die unterstützt, indem man auf praktische Art eingeführt wird."

„Hier ist alles offen und man will niemandem auf den Schlips treten."

5.3 Probanden/-innen und Beziehungspflege

Kontakt unter den Probanden/-innen und zu den Interviewenden

- … untereinander von herzlichen Umarmungen bis hin zu schweigsamen Runden, jedoch stets per „Du."
- In zwei Organisationen werden auch den Interviewer/-



innen das „Du“ unmittelbar nach dem Eintreffen angeboten.

Auftritt

- Hinsichtlich Kleidung wird quer durch alle Unternehmen und Unternehmensbereiche ein lockerer Stil gepflegt. Allerdings sind die Temperaturen an allen Explorationstagen sommerlich warm.

Vorabinformationen bzw. Erwartungen

- Beim Warming-up vor der ersten Test-Spielrunde wird in allen Organisationen eine erwartungsvolle, produktive Spannung gewahr. Die verantwortlichen Kontaktpersonen der beiden Testgruppen (Awareness-Verantwortliche), mit denen anschließend je eine Gruppendiskussion stattfindet, wurden gebeten, den Teilnehmenden vorab „nicht zu viel“ zu verraten, d. h. es wurde kommuniziert, dass es sich um eine Veranstaltung der Informationssicherheit handelt, aber keine weiteren Details bekannt gegeben.
- In einem Unternehmen mischt sich jedoch auch Enttäuschung in breiter Front hinzu, da man darauf gehofft hatte, dass der dort herrschende restriktive Umgang mit Online-Zugängen gelockert werden würde und die Veranstaltung als Schulung konkret darauf vorbereiten soll. Daher kommt man hoch motiviert mit Stift und Schreibblock im Anschlag zum Test. Hier war die Anspannung deutlicher spürbarer als in den anderen Unternehmen:

> *„Schade, und ich dachte, ich könnte ab morgen an meinem Arbeitsplatz frei surfen ….“*

In dem als besonders entspannt empfundenen Unternehmen berichtet der IT-Leiter, dass er den Mitarbeitenden eine „Wellness-Veranstaltung“ angekündigt hatte.

Und während diese im Konferenzraum eintrudeln, wird mit zahlreichen Scherzen bzw. feiner Ironie tatsächlich auch eine lockere Wohlfühlatmosphäre geschaffen.

> *„Wir sind sehr sicher, unser Admin wuppt das schon.“*

Nachwirkende Beziehungspflege …

- … von Kommunikationsabrissen nach dem Test bzw. der Befragung über explizite Dankes-Mails bis hin zu Anforderungen eines Kostenvoranschlags für LS der „Security Arena.“

> *„Danke, Sie haben einen bleibenden Eindruck hinterlassen. Heute wurde mir noch einmal gespiegelt, dass die Teilnehmerinnen und Teilnehmer großen Spaß an der Veranstaltung hatten und gleichzeitig eine Menge gelernt haben. Können Sie mir bitte noch einmal mitteilen, wie die drei Spiele genau heißen?“*

5.4 Zwischenfazit

Bei allen Gemeinsamkeiten und insbesondere in Bezug auf den hohen Bedarf an Sicherheitskommunikation wird deutlich – ein KMU ist nicht 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 die Sicherheitskultur (Definition s. Grundlagenstudie [2], S. 13) und bezüglich Security Awareness bzw. die Nutzung von Gamification (Definition s. Grundlagenstudie [2], S. 39) bedingen.

Während die kulturellen Ausprägungen in Großunternehmen offenbar infolge relativ ähnlicher Konzernstrukturen bzw. sich immer stärker nivellierender Prozesse sich auch hinsichtlich von Sicherheitskulturen anzugleichen scheinen, wirken in den befragten KMU – auch infolge psychologischer Verstrickungen (s. Grundlagenstudie [2], S. 31ff.) – deutlich ausdifferenziertere Sicherheitskulturen.

Ausgehend von der Annahme, dass in kleineren KKU (Kleinst- und Kleinunternehmen mit weniger als 50 Mitarbeitenden) sowie in abweichenden Branchen nochmals abweichende kulturelle Verhältnisse gelebt werden als in den von hier evaluierten mittleren Unternehmen, erscheint die sicherheitskulturelle Bandbreite, für die im Projekt „ALARM Informationssicherheit“ Sensibilisierungswerkzeuge kreiert werden sollen, enorm hoch.

Im Zuge dieser sehr breiten Ausdifferenzierung agieren manche mittlere Unternehmen in Bezug auf Sicherheits- bzw. Unternehmenskultur ähnlich wie Konzerne oder andere Großunternehmen und andere wiederum wie z. B. Einzelhändler oder Einzelunternehmen. Gerade auch in den beiden hier per Gruppendiskussion befragten Testunternehmen waren jeweils extreme Ausprägungen hinsichtlich des Reifegrads von Sicherheitskultur generell nachweisbar (mehr hierzu in Kapitel 7).

Insbesondere der Grad der Digitalisierung mit der – je nachdem – Förderung oder Verhinderung digitalisierter Prozesse, mit beschränkten bzw. unbeschränkten (Online-)Zugängen von Mitarbeitenden zeigt die enorme Spannbreite, in der KMU vor dem Hintergrund einer immer höheren wirtschaftlichen Komplexität agieren.

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. Der auf Differenzierung spekulierende modulare Ansatz aller hier getesteten LS mit der individuellen Adaptierbarkeit unterstützt jedoch dabei, diese große Bandbreite auszubalancieren.


Sicher zuhause wohnen & arbeiten

6. Wirkungsanalyse der Lernszenarien, ihrer Gestaltung und Usability

6.1 Wirkungsanalyse der Lernszenarien

6.1.1 Sicher zuhause wohnen & arbeiten

Dieses LS ist das mit den wenigsten Störstellen und funktioniert ähnlich wie bereits bestehende LS der „Security Arena“, die Wimmelbilder als Lernkarten-Spielfeld sowie so genannte „Risikokarten“ und „Schutzkarten“ einsetzen („Sicher unterwegs“, „Fallstricke am Arbeitsplatz“, „Car Security“, „Operational Technology Security“). Das Spielprinzip muss nicht ausschweifend erklärt werden, sondern wird nach wenigen Sekunden wie von selbst verstanden. Mit den zum größten Teil vertrauten Risiko-Szenarien wird dieses LS als idealer „Soft-Einstieg“ in einen Lern-Parcours zum Thema Informationssicherheit erlebt – wie es sich im folgenden Zitat widerspiegelt:

„Das ermöglicht Erfolgserlebnisse, man fühlt sich nicht total hilflos.“

Man ist dankbar, die eigene Erfahrung mit dem Homeoffice, die infolge der Pandemie beschleunigt wurde, noch einmal in Bezug auf Informationssicherheit und Datenschutz aufarbeiten und dabei betriebliche und private Themen zusammen thematisieren zu können. Z. B.:

„Das ist ja wie im richtigen Leben – da liegen Videokonferenz mit dem Chef und das Weinen der Kinder auch eng beieinander.“

Auch andere Rückmeldungen drücken aus, dass das Spiel als alltagsnah erlebt wird:

„Eigentlich ist das alles klar und trotzdem passiert es einem.“

Viele Mitarbeitende tauschen sich über Beispiele aus dem eigenen Umfeld aus, jüngere führen vor allem solche an, die den eigenen Eltern oder Großeltern passiert sind. Aufgrund des Herumlavierens mit entsprechend ambivalenter Körpersprache entsteht bei denjenigen Teilnehmenden, die ihre Verwandschaft als größte Risikogruppe auszumachen versuchen, der Eindruck, man wolle sich gegebenenfalls mit eigenen Unzulänglichkeiten hinter Dritten verstecken.

Gelächter wird durch die Idee von „Alexa auf der Toilette“ (Szenario 5) ausgelöst. Es wird in lebhaftem Gespräch und zugleich zügig gespielt. Z. B. wird erzählt, dass eine Schulung zum Homeoffice vor einigen Jahren zu starken Ängsten geführt habe, vor allem im Hinblick auf Passwörter, die gegebenenfalls mit der Familie geteilt werden. Oder hält man diese Angst von sich fern, indem man, – wie oben erzählt – „die ältere Generation“ als bedeutendste Zielgruppe von Social Engineers vermutet? Eine Mitarbeiterin erzählt z. B. sehr anschaulich von einer falschen Handy-Rechnung, die ihr Vater erhielt und um die sie sich in einer langwierigen Prozedur kümmern musste.

Es wird in einem Unternehmen aber auch berichtet, dass selbst bei hohen Inzidenzzahlen während der Pandemie kein Homeoffice erlaubt gewesen sei und erwartet wurde, dass man auf der Arbeit zu erscheinen habe. Dabei scheint ein Bedauern mitzuschwingen, sich dem Virus-Risiko ausgesetzt haben zu müssen. Andererseits wird dort aber auch relativiert, die Motivation zur Arbeit sei im Büro höher. Hierbei entsteht der Eindruck, dass man in Anwesenheit des IT-Leiters nicht wagt, sich kritisch zu der Situation zu äußern, dass in diesem Unternehmen Homeoffice selbst bei hoher Corona-Inzidenz nicht erlaubt war und auch heute – mehr als zwei Jahre nach Beginn der Pandemie – noch nicht vorgesehen ist.

Die richtige Zuordnung der 34 Karten zu den 17 Szenarien gelingt in allen Fällen relativ schnell. In der Regel reichen die 5 Minuten Spielzeit aus, ohne dass hinsichtlich dieser vermeintlichen Limitierung zu einem schnelleren Agieren motiviert werden musste. Bei einer Testgruppe wurden die Unterschiede der Szenarien 2 (ungesperrter Rechner) und 3 (Passwortnotiz) sowie 16 (Einblicke in die Privatsphäre) und 17 (Abschaltung VPN) erst nach differenzierter Erklärung durch den Moderator verstanden. Es bleibt jedoch bei diesem Einzelfall.

In der Nachschau wird die Wichtigkeit des Themas betont und die Umsetzung gelobt, das Spiel dieses LS als relativ „leicht lösbar“ und „extrem praxistauglich“ bewertet. Aus Sicht der Evaluation gibt es keinerlei Änderungsbedarf.

6.1.2 Kundendaten sicher managen in Cloud & Co.

Dieses LS wird in der Kombination der Themenschwerpunkte nicht hinreichend verstanden. Das Thema Passwort wird zwar von allen Beteiligten als ungemein wichtig erachtet. So geraten Spielteil 1 (Passwort) und die Diskussion um das Passwortranking sehr lebhaft. Bei den anderen beiden modularen Spielteilen wirken die Teilnehmenden jedoch seltsam blass und wenig involviert und geben diesbezüglich auch ihren Unmut preis:

„Das ist auf Dauer ein bisschen langweilig, bei einer solchen Textlastigkeit schalte ich irgendwann ab.“

„Verstehe den Mehrwert nicht. Das sind doch nur Phrasen.“


CEO FRAUD
BUSINESSE-MAIL COMPROMISE (BEC)
CHEFE FAKE PRESIDENT SCAM
ENDE

Auch die interviewten Awareness-Verantwortlichen lehnen die Zusammenstellung des hiesigen Themencluster ab.

„Das sind alles wichtige Themen. Aber nicht glücklich kombiniert. Wenn schon eine Kombi, würde es besser zu Multifaktor-Authentisierung passen."

„Der zweite Faktor ist wichtig – ohne diese Verstärkung ist das Passwort-Thema unvollständig."

„Die Sicherheit in einer Cloud hängt doch für den normalen Anwender von einer ‚starken' Authentisierung ab. Daher ist Cloud für mich eh ein reines Passwortthema."

„Welche Cloud ich auswähle und das Drumherum – interessiert den Mitarbeiter doch gar nicht. Das ist letztlich Angelegenheit der Entscheider aus Geschäftsführung oder IT-Management."

Es wird empfohlen, dieses LS zu überarbeiten. Optimierungen betreffen insbesondere folgende Aspekte:

- Die Themen Kundendatenschutz und Cloud herausnehmen und entweder aus dem Themenportfolio streichen, an ein anderes Thema hängen oder ein eigenes Lernszenario, basierend auf beiden, aufmachen, z. B. Ersetzen der LS „Informationsklassifizierung" durch das Thema „Datenschutz".
- Dafür das Thema „Multifaktor-Authentisierung" (MFA) an das Passwortthema hängen und ins Spiel integrieren.

6.1.3 Die 5 Phasen des CEO Fraud

Dieses LS weckt Neugier, löst lebhafte Diskussionen aus, scheint aber zum Teil auch manche zu überfordern. Vor einem der Testläufe, bei dem man in der Vorbesprechung um Präfenzen hinsichtlich der finalen Auswahl mit drei LS für den Test bat, wurden 4 der 6 Test-LS aufgebaut. Als einzige LS wurde diese von den lokalen Moderierenden spontan nach relativ kurzer Betrachtung aussortiert.

Dabei wird die Relevanz des Themas unterschiedlich betrachtet. Die einen – vor allem auch die für Informationssicherheit bzw. Security Awareness zuständigen Kolleginnen und Kollegen – finden, dass CEO Fraud ein wichtiges Thema sei, bei dem einzelne Prozessschritte für beinahe alle Mitarbeitenden wichtig werden könnten, für andere ist dieses LS mehrheitlich eines für spezifische Zielgruppen mit entsprechenden Rechten, z. B. Mitarbeitende aus Buchhaltung oder Personalabteilung, gegebenenfalls auch für Geschäftsführende.

Es ist vor allem die Anzahl der Spielkarten, die zu groß, zu unüberwindbar erscheint, um den Prozess in der vorgegebenen Zeit mithilfe der Karten richtig auszulegen. Dabei stört, dass viele der Spielkarten an verschiedenen Stellen innerhalb der Prozesskette platziert werden können.

Erleichterung verschafft z. B. die den Anspruch senkende Information des Moderierenden, dass es ausreichen würde, die Spielkarten lediglich den fünf Prozessbereichen zuzuordnen. Dabei sind die Diskussionen während und nach dem Spiel sehr lebendig und belegen das Interesse am Thema und den damit verbundenen und hier ebenfalls thematisierten Kollateralrisiken, z. B. Profiling via Social Media, Social Engineering, Phishing.

In der anschließenden Gruppendiskussion berichtet ein Proband, er habe sich von dem Thema CEO Fraud *„wenig berührt gefühlt und mangels Rollenpassung"* die Vorstellung gehabt, *„auf den unteren Etagen hat man damit wenig zu tun."* Dadurch entsteht eine lebhafte Auseinandersetzung darüber, inwieweit Mitarbeitende mit geringem Rechte-Portfolio von dem Thema betroffen sind und wie sinnvoll bzw. risikoreich es z. B. sei, Kontaktdaten oder persönliche Vorlieben online abzubilden.

Als Wermutstropfen wird im Nachgang angeführt, dass z. B. im Gegensatz zum LS „Sicher zuhause wohnen & arbeiten" die eigentlichen Präventionsmaßnahmen zu kurz kämen. Es wird vehementes Interesse daran geäußert, wie man z. B. in der so genannten „Testing-Phase", eines der auf den Karten abgebildeten Prozessschritte, erkennen kann, bereits als Opfer eines CEO Fraud ausgewählt worden zu sein, um den eigentlichen Betrug gegebenenfalls rechtzeitig verhindern zu können. Eben:

„Bevor das Kind in den Brunnen gefallen ist …"

„Ich hätte gerne häufiger gewusst, was ich gegen die Einzelrisiken in den Vorbereitungen zum eigentlichen Betrug unternehmen kann."

In einem Unternehmen wird die Vermutung angestellt, dass es von Vorteil sein könnte, ein relativ kleines Unternehmen zu sein, weil man die persönlichen Eigenheiten der Kolleginnen bzw. Kollegen kenne, also Fremde besser einschätzen könne.

Dabei werden die Zusatzinformationen am Rand des Spielfeldes als hilfreiche Annotationen gewertet, vor allem aber das Gesamtbild mit diesen Infografik-Elementen zuzüglich des eigentlichen Prozess-Bildes mit den Spielkarten jedoch als erschlagend wahrgenommen.

„Das war auch mein Gefühl, dass mehr in diese Richtung bei uns einschlägt",

sagt eine Mitarbeiterin aus dem Personalwesen über die Infografik, die besagt, dass der HR-Bereich mit 25% zweitgrößtes Einfalltor nach dem Finanzbereich ist.


> 12 MRD. $
SCHADENSSUMME
WELTWEIT PRO JAHR
50 %
SCHADEN DER GESAMTEN
CYBERKRIMINALITÄT
E-MAIL-THEMEN
53 MIO. €
40 MIO. €
START
ENDE

Eine Testperson stellt hinsichtlich des Verlustes eines bekannten Autozulieferers infolge von CEO Fraud 2016 fest:

„Boaah, 40 Millionen Verlust in nur einem Fall, das hätte ich nie geglaubt. Dachte immer, dass sich sowas im unteren fünfstelligen Bereich abspielt."

Ein dennoch fühlbarer Rest an Reaktanz im Kontext der Zustimmung zu diesem LS könnte mit den hier beeindruckend hohen Summen zu tun haben, die offenbar Ängste auslösen, aber auch mit eigenen Fällen der nahen Vergangenheit, von denen alle hier beteiligten Unternehmen bzw. Probanden/-innen berichten können:

„Ich habe am Ende nur daher nicht auf die scheinbare E-Mail meines Chefs reagiert, weil mir seine Grüße in der besagten E-Mail zu formal ausgefallen waren – das war einfach nicht seine Sprechweise, daher habe ich ihn nochmal kontaktiert, auch wenn das sehr zeitaufwändig war."

„Ja, kennen wir. Schon mehrfach. Aber da will ich nicht mehr drüber reden."

In einigen Fällen wird die Delegation an eine bestehende Cyber-Versicherung als wichtiger angesehen als die notwendige Awareness:

„Wir hatten so einen Fall vor knapp zwei Wochen. Niedriger fünfstelliger Betrag. Das Geld ist wohl weg. Zum Glück haben wir eine Cyber-Versicherung – die zahlt."

Der zweite Teil des Spiels, die Zuordnung von 6 Phishing-Karten in „Phishing" vs. „Non-Phishing" kann in sämtlichen Tests nicht realisiert werden, da aufgrund lebhafter Diskussionen im Kontext des Prozessbildes aus Teil 1 die Zeit dafür fehlt. In der Nachschau wird auf die Information, dass eigentlich ein zweiter Spieleteil vorgesehen war, mit Ablehnung reagiert:

„Braucht keiner – das Hauptspiel ist schon komplex genug."

Es wird empfohlen, dieses LS zu überarbeiten. Optimierungen betreffen insbesondere folgende Aspekte:

- Reduktion der Spielkarten oder Vereinfachung des Gesamtprozesses im Spiel und/oder gegebenenfalls auch der Spielregeln (z. B. Zuordnung lediglich zu den fünf Prozesshauptschritten)
- Gegebenenfalls Integration von Präventionsmaßnahmen in den unmittelbaren Spieleprozess statt ausschließliche Awareness-Anreicherung via Moderations-Briefing
- Gegebenenfalls Streichung des zweiten Spielmoduls „Phishing"

6.1.4 Mobile Kommunikation, Apps & Co.

Dieses LS funktioniert ähnlich wie das LS „Sicher zuhause wohnen & arbeiten" und bereits bestehende LS der „Security Arena", die Wimmelbilder als Lernkarten-Spielfeld sowie so genannte „Risikokarten" und „Schutzkarten" einsetzen. Beim Spielen entsteht ein recht angeregter Austausch über Beispiele von Ausspähen von Bank- und Kontaktdaten. Die Detailerfüllung der Aufgaben scheint als recht schwierig und doch involvierend erlebt zu werden. Die Probanden /-innen wirken trotz der längeren Spieldauer im Verhältnis zum Wimmelbild aus der LS „Sicher zuhause wohnen & arbeiten" sehr konzentriert.

Die höhere Komplexität ist dabei offenbar darauf zurückzuführen, dass die verschiedenen Szenarien als sehr ähnlich erlebt werden. D. h. im Gegensatz zu den anderen Wimmelbild-basierten Stationen lassen sich die Risiken visuell nicht so eindeutig differenziert abbilden. In vorahnender Bewusstheit dieser Barriere wurden auf dem hiesigen Spielfeld die Szenarien von den Produzierenden verdoppelt. Sprich: neben den üblichen Darstellungen von Real-Life-Szenarien, in denen die Handelnden ihre Smartphones benutzen, sind diesen jeweils Hände mit den zugehörigen Smartphone-Screenshots zugeordnet, um das jeweilige Risiko relativ schnell identifizieren zu können. Die Darstellung von Figuren als Handelnde wäre nicht ausreichend, wenn diesen nicht zusätzlich auch Sprech- oder Denkblasen mit Texten zugeordnet wären, die das Handeln bzw. die einzelnen Risiken kommentieren. Manche Teilnehmende realisieren die jeweiligen Passungen von Szenario, Sprech- oder Denkblase und Hand mit Smartphone-Screenshot dennoch erst nach mehrfachen Hinweisen durch den Moderierenden. Trotz dieser eher redundanten Visualisierung und der ergänzenden Hilfestellung durch die Moderation fiel die Zuordnung der Spielkarten in mindestens einem KMU relativ schwer:

„Es ist gar nicht so eindeutig, wo diese Karte jetzt hinkommt – die passt ja zu mehreren Bildern."

Die Zuordnung verläuft aus den oben genannten Gründen in dem besagten Unternehmen konzentrierter und schweigsamer, so dass der beabsichtigte Diskurs sich während des Spiels nicht auf dem lebendigen Niveau anderer Wimmelbild-basierter Stationen einpendelt. Im Nachgang des Spiels lebt die Auseinandersetzung jedoch wieder auf. Das Thema wird als sehr wichtig erachtet.

Weitere Störstellen wurden nicht evaluiert, so dass das eher zurückhaltende Spielen keinen direkten Einfluss auf die Gesamtqualität des Diskurses im Kontext dieses LS ausübt. Insgesamt läuft dieses LS nicht so flüssig ab wie


Georgia
ALERT
U-BAHN
known_sense

„Sicher zuhause wohnen & arbeiten“, jedoch besser als die meisten anderen getesteten LS – mit Ausnahme des LS „Cyber Pairs“ (s. unt.).

Eine Awareness-Verantwortliche, die das bisherige, ältere LS zu diesem Thema aus der „Security Arena“ kennt, würde jedoch die bisherige Station der neuen vorziehen und meint:

„Die neue sieht schon interessant aus, aber ganz ehrlich: die alte App-Station der ‚Security Arena‘, die wir lizenziert haben, gefällt mir deutlich besser.“

Es wird empfohlen, dieses LS zu überarbeiten. Optimierungen betreffen ausschließlich eine transparentere Darstellung bzw. Zuordnungsoption der Doppelbilder (Personen bzw. Hände mit Smartphones und Screenshots) auf dem Spielfeld. Gegebenenfalls könnte überlegt werden, zusätzlich in den Texten der Spielkarten Anker zu setzen, die nach der Erfassungsmethode des Querlesens als Schlagwörter funktionieren, indem sie mit Sprechtexten auf dem Spielfeld korrelieren – auf diese Weise konnten in der LS „Sicher zuhause wohnen & arbeiten“ zahlreiche Karten beinahe beiläufig zugeordnet werden, ohne die Kartentexte vollständig zu lesen bzw. kognitiv zu verarbeiten.

6.1.5 Cyber Pairs

Dieses LS polarisiert ungemein. In einem Unternehmen sind selbst dem IT-Leiter nicht mehr als zwei Begriffe bekannt, dem Rest der Teilnehmenden gar keiner – eine Situation, die trotz aller moderierenden Animation zu schüchternen und zum größtenteils beklemmend schweigsamen Zusammenführungen von Fragmenten nach dem Prinzip „Trial & Error“ führt, deren Ergebnisse in der Regel unrichtig waren.

„Ich komme mir voll dumm vor“,

gibt jemand schließlich zu, begleitet von lauten Lachern der anderen Teilnehmenden.

„Da kommt mein Latein ja doch noch mal zum Einsatz“,

freut sich jemand, der einen Begriff übersetzen kann.

Beispiele zu den meisten Begriffspaaren, z. B. im Sinne von Vorfällen bzw. Incidents, können aber nicht genannt werden.

In einer anderen Gruppe wird so kontrovers diskutiert, teilweise über als *„schräg“* empfundene Wortkobinationen gelacht, dass es dem Moderierendem kaum gelingt, dazwischen zu kommen.

„Super interessant“,

wird in der anschließenden Gruppendiskussion betont. Oder:

„Da waren viele Begriffe, die ich noch nicht kannte, die aber gut zu wissen sind. Ich wusste bisher nicht, warum ich zuhause Briefe schreddere – jetzt weiß ich es.“

„Das ist wie ein Anker. Ich kenne jetzt die Begrifflichkeiten und würde jetzt z. B. einen Artikel über einen der Begriffe lesen, weil ich jetzt zumindest einen Anhaltspunkt habe.“

„Man merkt, dass es nicht um Intelligenz geht, dass das jedem passieren kann, man muss sich nicht schämen. Sonst entschuldigt man sich ja zum Teil schon dafür, fragen zu müssen.“

Es kommt während der anschließenden Gruppendiskussion der Vorschlag auf, das Cyber-Pairs-Spiel in zwei Teile zu teilen, weil es „so ungemein viel Input“ beinhalte:

„Es ist einfach wichtig, die Erklärungen zu bekommen.“

Da jede Kombination und jedes richtig zusammengesetzte Paar in Bezug auf Definition, praktische Begegnung im Unternehmen oder privat, mögliche Popularität in den Medien und viele andere Aspekte besprochen wird, dauert dieses LS bei einem der Unternehmen knapp 40 Minuten. Der Spielablauf wird spontan mit den positiven Seiten des Vokabeln-Lernens in der Schule assoziiert. Hinweise, dass wir die anderen beiden Test-Stationen gegebenenfalls streichen müssten, werden weg gewischt mit dem Argument, man wolle nun jetzt alles, wenn es schon so spannend wird, genau unter die Lupe nehmen.

Es sind Begriffspaare wie „Quid pro quo“ oder „Ransomware“, bei denen vor allem auch private Bezüge hergestellt werden, außerdem sind „CEO Fraud“ oder „Deep Fake“ durchaus bekannt und können teilweise auch erklärt werden. Die Erklärung des Kompositums „USB Dropping“ gelingt erst im dritten Versuch und löst einen lebhaften Austausch und gegenseitige Erklärungen innerhalb der Gruppe mit Beispielen von inszenierten Awareness-Pentests mit potenziell „verlorenen“ USB-Sticks auf einem Parkplatz aus.

„Die arrangieren ‚verlorene‘ USB-Sticks im Unternehmensumfeld. Ach, du meine Güte. Wird so etwas wirklich als Awareness-Maßnahme verkauft?“,

... fragt eine Testperson. Und:

„Für mich ist sowas ein Vertrauensbruch – das geht gar nicht.“

Auch das Memo-Paar „Social Engineering“ fasziniert, kann aber fachlich nicht zufriedenstellend erklärt werden:


Halle 14

„Das ‚social' klingt ja eigentlich ganz nett",

meint die Wortführerin einer Gruppe.

„Wir sind so gut geschützt, wir können das gar nicht",

schmeichelt die Wortführerin dem anwesenden IT-Leiter.

Ein besonders lebhafter Austausch gelingt im Kontext des Angriffsvektors „Spear Phishing." Es wird in aller Breite diskutiert, ob die Darstellung des Teams mit persönlichen Kontakten auf der eigenen Website in diesem Zusammenhang nicht ein zu hohes Risiko darstellt, auch wenn der persönliche Kontakt zur Kundschaft und zu den Lieferunternehmen als Teil der eigenen Unternehmenskultur verstanden wird.

Dabei wirken die Probanden/-innen äußerst wissbegierig und stellen den beiden anwesenden IT-Experten Fragen, z. B.:

„Warum ist es eigentlich so schwer, sich vor Ransomware mit einer Firewall zu schützen?"

Dabei scheinen die Teilnehmenden von der Heterogenität der Gruppen zu profitieren. Denn die beiden ITler gehen gerne und zum Teil ausführlich auf die Fragen ein, und es entwickelt sich ein Gespräch über den „menschlichen Faktor." Je länger diese Diskussion dauert, je mehr Begriffspaare thematisiert werden und je detaillierter in diesem Kontext interne Prozesse angerissen werden, umso mehr scheint das Gefühl zu schwinden, tatsächlich gut geschützt zu sein. Das gemeinsame Werk, die Begriffe und deren Abwehroptionen zu thematisieren, entschädigt jedoch für die gefühlte Unsicherheit. Allein der Aufwand des mühsamen miteinander Durchkauens scheint eine Art Kitt für die vorhandenen Vakanzen zu sein. Am Ende ist man froh, sich gegen alle Widerstände durchgekämpft zu haben.

Bei diesem LS fällt sehr deutlich der Unterschied zwischen unbewusster und bewusster Inkompetenz ins Auge. Die zuletzt beschriebene Gruppe stammt aus einer Organisation mit einem als potenziell höher einzuschätzendem Reifegrad in Bezug auf die Sicherheitskultur generell. Kompetenzlücken werden hier als ein berechtigter Mangel wahrgenommen, der zu füllen ist, und nicht als persönliche Scham, unwissend und damit quasi „nackt" dazustehen. Eine derartig souveräne Position erfordert einen permanenten Diskurs zum Thema. Man könnte also behaupten, dieses LS ist weniger für KMU geeignet, die eher unsichere Awareness-Beginner bespielen wollen, sondern für eine bereits vorsensibilisierte Zielgruppe, die die Spielintention als Aufforderung versteht, den Reifegrad im Sinne einer bewussten, dynamischen Weiterentwicklung von u. a. Awareness über eine gemeinsame Auseinandersetzung zu verbessern.

Deutlich wird aber auch: Diesem LS, das ausgezeichnet in Organisationen mit höherer Reife funktionieren sollte, ist ein Zeitproblem inhärent. Die Risiko- und Schutzkarten wurden so gut wie gar nicht auf die Vertiefungen der Rückseiten gedreht – dafür fehlte schlichtweg die Zeit. Die Kernspielzeit ist mithin nicht passend kalkuliert und auch die Gesamtzeit von 15 Minuten reicht nicht aus, um alle 16 Begriffspaare ausreichend zu thematisieren.

Es wird aber auch deutlich, dass nicht für alle hier thematisierten Risiken reale Schutzeinflüsse bei den Mitarbeitenden vorhanden sind. Z. B. beim Angriffsvektor „DDoS Angriff" sind letztlich vor allem Sicherheits- bzw. IT-Protagonisten/-innen für die Abwehr zuständig, weniger die Mitarbeitenden selbst. Auch bei anderen, auf den Karten beschriebenen Schutzmaßnahmen kommt es zu Redundanzen, insbesondere dann, wenn es darum geht, Phishing und die damit verbundenen mannigfaltigen Ausprägungen abzuwehren.

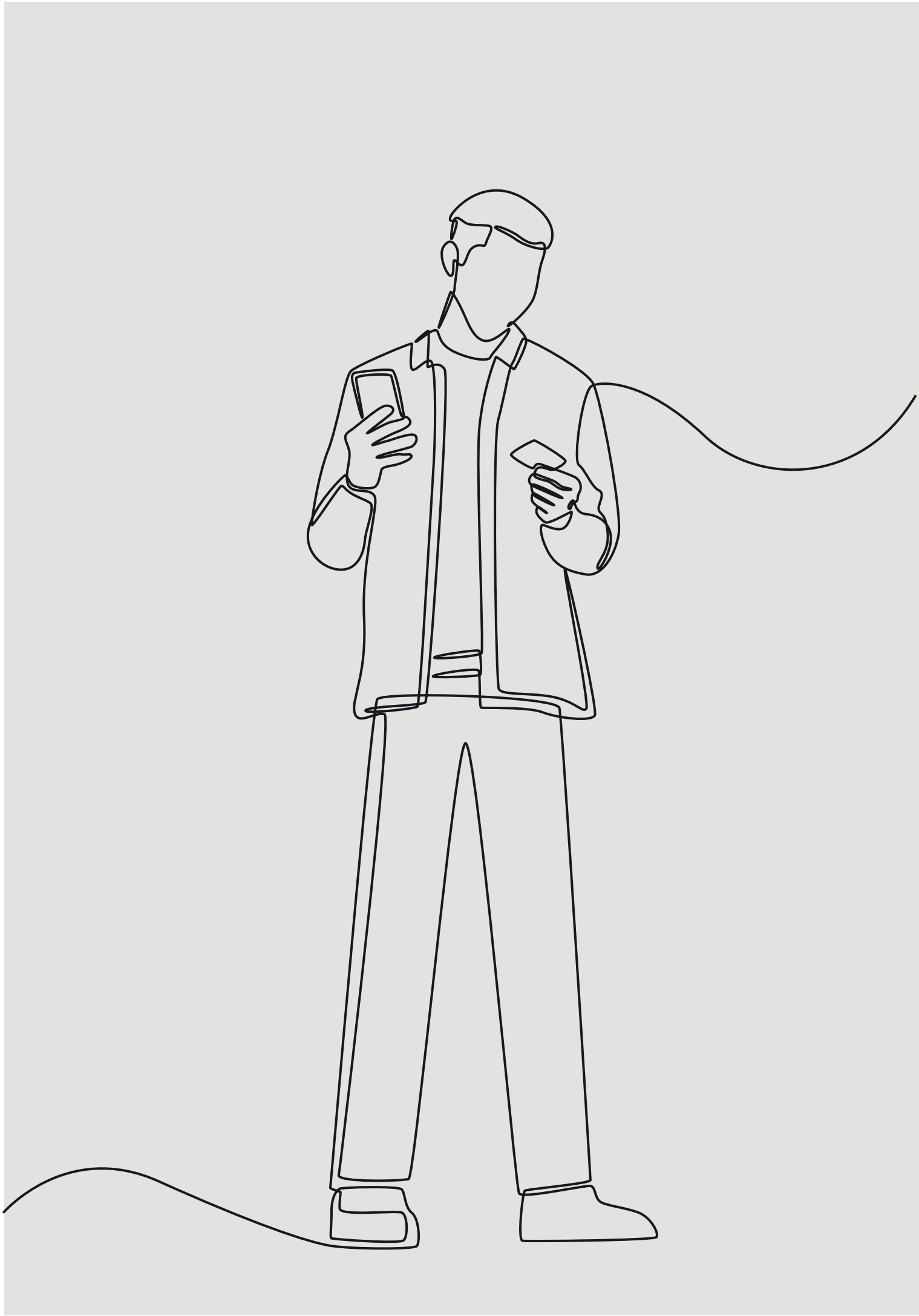
Es wird empfohlen, dieses LS zu überarbeiten. Optimierungen betreffen insbesondere folgende Aspekte:

- Rückseiten bei den Risiko- und Schutzkarten weglassen, gegebenenfalls Inhalte auf Vorderseite durch kurze Ergänzungen erweitern.
- Optional die Rückseite nutzen, jedoch nicht offensiv hinsichtlich des Spiels kommunizieren, sondern allenfalls bei Bedarf als zusätzliches Informationsmaterial beim Debriefing durch die Moderation nutzen lassen, indem diese die benötigte Definition durch Umdrehen der Karte vertieft.
- Gegebenenfalls Schutzkarten ersetzen durch ein Spielfeld mit 5–6 verschiedenen Boxen, die für die wichtigsten Schutzmaßnahmen stehen und denen die Begriffskarten zugeordnet werden sollen, denn nicht alle Schutzmaßnahmen unterscheiden sich im Detail voneinander.
- Im Moderations-Briefing deutlich herausarbeiten, dass gegebenenfalls 8–10 Begriffspaare (und damit nur 16 bis 20 Karten) für die vorgegebene Spielzeit ausreichend sind und damit eine Überforderung von vornherein ausgeschlossen werden kann.

6.1.6 Informationsklassifizierung

Es werden vom Moderierenden 30 typische Dokumentenarten aus den 50 beschrifteten Holz-Klötzchen ausgewählt. Ein Spielfeld mit Sortierboxen, wie es im Projekt geplant ist, steht noch nicht zur Verfügung. Dafür werden farbige Filzdecken mit Aufstellern und beschrifteten Klassenbezeichnungen eingesetzt.

Die Teilnehmenden sortieren die Dokumente (Klötzchen) in der Regel auf den vier Decken vor, bevor sie damit beginnen, Türme daraus zu bauen. Das Material, nur geringfügig behandeltes Holz mit transparenten, selbstklebenden Beschriftungsbänden, wird als hochwertig wahrgenommen. Mehrfach streichen die Teilnehmenden sanft ihre Hände über die Oberfläche, ein stiller Hinweis auf die Wichtigkeit von Haptik bei LS und Awareness-Materialien generell.



Das Bauen wird nur zögerlich begonnen und ausgeführt. Jedes Holzklötzchen wird ein zweites Mal auf Passung untersucht und besprochen. Obwohl vom Moderierenden Zeitdruck entwickelt wird, um das Spiel in der vorgesehenen Zeit zu beenden, ist Reaktanz spürbar, die Klötzchen final zu verbauen. Im Big Picture eines Turms erscheinen die Bausteine den Teilnehmenden offenbar unwiederbringlich, d. h. ohne Korrekturmöglichkeit, verbaut. Dadurch geht viel Spielzeit verloren, die jedoch durchaus produktiv mit Diskursen gefüllt wird.

Für die anschließende Zuordnung der Verwendungskarten bleibt jedoch keine Zeit mehr übrig. Die verlängerte Spielzeit hat aber auch mit dem mangelnden terminologischen Verständnis zu tun. Zahlreiche verbale Ansetzungen von Dokumentenarten auf den Holzklötzchen werden im ersten Zugriff nicht verstanden und müssen vom Moderierenden – oftmals langwierig mit mühevoller Akzeptanz der Teilnehmenden – erklärt werden:

„Was sind denn ‚Bedienungsanleitung komplexe Standardmaschine'?"

„Liste von Teilnehmenden ‚Informationssicherheits-Training' oder ‚Mitarbeitende-Zertifikat' – so spricht doch keiner."

Das Unwohlsein im Kontext der sprachlichen Ansetzung (z. B. gendergerechte Sprache mit z. T. komplexen Wortbildungen) sowie der vorausgegangene langwierige, mit zahlreichen Kommentaren angefütterte, komplexe Findungsprozess generischer Dokumentenarten, die idealerweise für beinahe alle KMU von Relevanz sind, führt zu einer Art eines babylonischen Turmbauprozesses mit Goldener-Mitte-Kompromiss, bei dem am Ende offenbar wenig verstanden wird und kaum jemand von den Probanden /-innen zufrieden zu sein scheint. Darüber hinaus wird in den Interviews mit den Awareness-Verantwortlichen deutlich, dass sie diese Station nicht nur wegen der unglücklichen Terminologie, sondern auch aufgrund des komplexen Handlings ablehnen.

„Sorry, völlig daneben, ich schleppe doch nicht ein paar Kilo Holzklötze durch unsere Standorte – diese Station hat mit der angeblich kinderleichten ‚Out-of-the-Box'-Logik nichts mehr zu tun."

Da bei einer anstrebenswerten Gewichtsreduktion mit einer Verkleinerung der Holzklötze von der Seitenlänge von 15 cm auf ungefähr 7–10 cm die Verwendungszweckkarten verkleinert werden müssten, damit man sie in die zu erreichtenden Türme einwerfen kann, müsste auch die Textgröße auf den Spielkarten stark verkleinert werden – auf Kosten der Lesbarkeit. Und eine Gewichtsreduktion durch leichtere Trägermaterialien hätte keinen Einfluss auf das als zu groß wahrgenommene Volumen, das aktuell die Verpackung der bisher größten LS (DIN A2-Grundfläche) deutlich übertrifft. In den Gesprächen mit den Awareness-Verantwortlichen wird jedoch auch klar, dass es sich bei dem Thema „Informationsklassifizierung" in KMU thematisch in vielen Fällen um eine Art Wunschkonzert handeln würde, das weit von der aktuellen Arbeitswirklichkeit entfernt ist. Einer stellt daher fest:

„Warum sollte ich eine Station Infoklassifizierung anbieten, wenn es keine Chance gibt, den Prozess bei uns real auszurollen – so weit sind wir noch lange nicht."

Der Widerstand ist mithin sowohl auf Seite der Teilnehmenden, als auch auf Seite der Awareness-Verantwortlichen erheblich. Es wird empfohlen, die Weiterentwicklung eines LS „Informationsklassifizierung" zu überdenken und das Thema gegebenenfalls zu ersetzen (z. B. durch das Thema Datenschutz respektive Informationsschutz allgemein) oder aber deutlich offener zu gestalten, z. B. indem der Fokus auf Informationen allgemein gelenkt wird statt beinahe ausschließlich auf Klassifizierung (z. B. Unterscheidung „Datenschutz" vs. „Informationsschutz, Wert von Informationen o. ä.).

Die in der Grundlagenstudie [2] genannten, favorisierten Themen mögen die Wichtigkeit von Informationsklassifizierung belegen – dies bedeutet aber nicht, dass bei den allen KMU der Reifegrad vorhanden ist, einen solchen Prozess auch zur Anwendung zu bringen. Falls eine Ersetzung nicht infrage kommt, sollte auf eine generische Ansetzung von Dokumentenarten verzichtet werden. In diesem Fall sollte lediglich das Moderations-Briefing und ein Spielfeld (DIN-A1) mit 4 Sortier-Boxen (DIN-A4) sowie Reitern zur individuellen Beschriftung der jeweils eigenen Klassennamen zur Verfügung gestellt und dazu aufgefordert werden, 25–30 DIN A4-Dokumente aus eigenen Beständen exemplarisch auszudrucken, zu nummerieren, zu laminieren und ins Spiel zu integrieren. Mithilfe typischer Dokumente aus dem eigenen Haus lässt sich das Thema weitaus anschaulicher gestalten. Dies könnte die Bindung an dieses LS und die Motivation, dieses auch einzusetzen, erhöhen.

6.1.7 Messenger, sichere Übertragung, Verschlüsselung

Dieses LS kann nicht angespielt werden, da zum Zeitpunkt der Feldarbeit lediglich ein Grobkonzept vorliegt. Die Idee, im Spielteil 1 diversen Messengern verschiedene Risiken zuordnen zu lassen, wird von den Awareness-Verantwortlichen in den Fokus-Interviews durchaus positiv beurteilt. Allerdings wird bezweifelt, dass das Spiel ohne eine juristisch nicht umsetzbare Nutzung konkreter Anbieter-Logos ausreichend attraktiv wäre. Teil 2 des Spielkonzeptes, das Thema Verschlüsselung über ein Tool, z. B. „Cäsarscheibe", zu erklären, wird konsequent abgelehnt. Begründet wird dies u. a. wie folgt:


Mobile Kommunikation, A
Data processing site
Georgia
ALERT
Darf «Café Cortina» auf deinen Standort zugreifen?
Mit dem Sie damit über interessante Aktionen und Angebote informieren.
Beim Verwenden der App
Immer erlauben
Nicht erlauben
Passwort falsch
Bitte erneut versuchen
Communication Data
BUY
INSTALL
Diese neue Gesundheits-App ist schon klasse. Aber Moment mal? Wo sind meine Daten gespeichert? In Georgien?
Mist, hab' ich mir irgendwas eingefangen?
Mama, hab Hunger!
known_sense

„Die müssen, ja sollen doch gar nicht verstehen, wie Verschlüsselung funktioniert, sie sollen lediglich dafür sorgen, dass eine sichere Übertragung stattfindet. Dafür ist die Tool-Auswahl entscheidend. Wie ein Tool genau funktioniert, das verschlüsselt, ist doch letztlich egal und dem User völlig piepe."

„Cäsarscheibe (?) - hübsche Idee aus Sicht des Spielentwicklers, aber sonst nichts.

Es wird empfohlen, dieses LS und vor allem das Spiel auf das Thema „Messenger" zu beschränken. Die Idee, Verschlüsselung z. B. anhand einer Cäsarscheibe oder ähnlicher Werkzeuge demonstrieren zu wollen, zu streichen, auch wenn es den spielerischen Mehrwert einer Simulation potenziell deutlich anheben würde, und auf Logos bestehender Produkte wegen der juristischen Unsicherheit in Bezug auf Nutzungsrechte konsequent zu verzichten.

Themen wie „sichere Übertragung" könnten über das Moderations-Briefing in den erwünschten Diskurs integriert werden. Als unkritisch wird ein Spiel mit einer Bewertungsmatrix eingeschätzt, die zwar die Bezeichnungen bestehender Messenger nutzt, nicht aber deren Branding-Elemente, z. B. Logos.

6.2 Evaluation der Methode, der Usability und des Designs der LS

Die getesteten LS aus dem Projekt „ALARM Informationssicherheit" funktionieren methodisch einwandfrei; sie fügen sich generell auch gut und ohne weitere Abstriche bzw. große Auffälligkeiten in ein Gesamtportfolio mit älteren LS der „Security Arena" ein:

- Die Methode, eine Station in 15 Minuten mit einer Dreiteilung „Briefing-Spiel-Debriefing" abzuwickeln, funktioniert – auch modulare Skalierungen mit Nutzung in zeitunkritischen Langtrainings sind bei allen Themen möglich, das LS „Cyber Pairs" wurde 40 Minuten lang lebhaft diskutiert, ohne dass es in Bezug auf alle Details finalisiert ist.
- Signifikante Unterschiede bei der Nutzung der beiden ins Englische übersetzten Stationen, „Sicher zuhause wohnen & arbeiten" bzw. „Die 5 Phasen des CEO Fraud" zu den deutschen Versionen können nicht evaluiert werden.
- Das Selektieren der Teilnehmenden in Paare oder Kleingruppen, die während des Spiels zum Teil unabhängig und synchron agieren, funktioniert zum größten Teil in Selbstorganisation, d. h. ohne großes Engagement der moderierenden Person.
    - Selbst der dadurch potenziell entstehende Nachteil, dass man bei einer Aufteilung in Kleingruppen „nicht alles mitkriegt", wird billigend in Kauf genommen. Dies spricht dafür, die LS-Teams eher deutlich kleiner zu halten als das avisierte Maximum von 12 Personen pro Station.
- Es wird der Wunsch nach einer Art Handout – z. B. eine Seite pro LS-Thema – für die Teilnehmenden zur Vertiefung des Live-Formats formuliert:

„Zum Beispiel um die vielen Infos nachzubereiten, etwa wie die Lösungsblätter in den Moderatoren-Briefings."

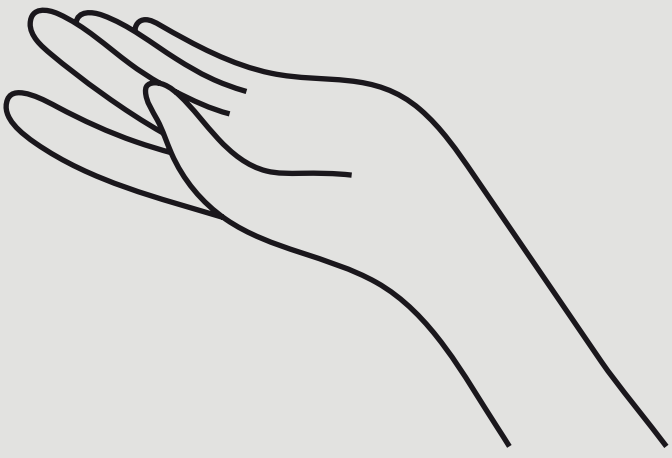
- Auch geben Security-fremde Führungskräfte, die zu den Stakeholdern der Informationssicherheit gehören, an, dass sie die hierüber kennengelernte Methode des Stationenlernens unterschätzt hätten und man darüber offensichtlich auch ihre eigenen Themenwelten, z. B. Personalmanagement, Change Management, Digitalisierung, an die Mitarbeitenden bringen könnte:

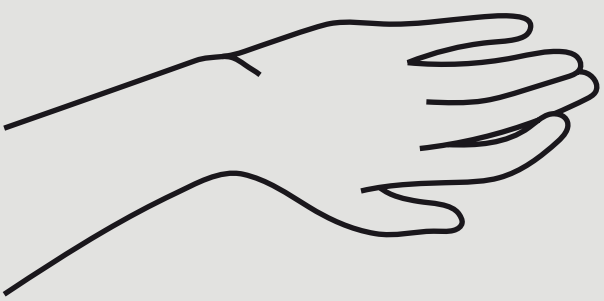
„Tolles Format, ich habe schon seit Jahren nach etwas gesucht, mit dem ich das Thema Digitalisierung in unserem Unternehmen beleben kann."

„Unsere Personalchefin war ja skeptisch, als ich ihr mitteilte, dass wir aus der Security spielerisch unterwegs sein werden. Aber jetzt hat sie Lunte gerochen und ich bin sicher, dass sie das Format künftig auch für HR-Zwecke nutzen wird."

Auch in Bezug auf die Gestaltung gibt es keine oder kaum Störstellen:

- Die **Designelemente,** vor allem die Wimmelbildlogik mit den reduzierten Illustrationen bei zwei LS, aber auch die gewählten Icons in den anderen LS funktionieren im intendierten Sinne ohne ausschweifende, zeitaufwändige Erklärung und tragen offenbar visuell zum Verständnis bei.
- In Bezug auf die **Farbwelt** sind benachbarte oder verwandte Designelemente in der Hauptfarbe ALARM_blau bzw. Sekundärfarbe ALARM_lila sehr oft schwer voneinander zu unterscheiden. Eine breitere Ausdifferenzierung des Projekt-Farbspektrums bei den Sekundärfarben oder die Einführung einer Tertiärfarbgruppe für besonders differenzierte Grafiken wie z. B. die Wimmelbilder wäre vermutlich hilfreich.
- **Typografisch** existieren keine Barrieren die Lesbarkeit oder andere Nachteile betreffend. Die gewählte Schrift wird in zwei Fällen als „steif" bzw. „unmodern" bezeichnet. Die typografische Wahl wird aber generell als zweitrangig eingestuft.
- Das **Branding** mit den zahlreichen Logos aller Projektpartnerinnen und -partner wird von einigen Probanden/-innen als störend wahrgenommen wie folgende Zitate belegen sollen:





„Das wirkt schon aufdringlich – ein bisschen so wie die Hintergründe von Interviewzonen bei Fußballübertragungen."

„Soll wohl zeigen, wie wichtig das ist, aber wenn wir das einsetzen sollten, hätte ich gerne eine Art Blankoversion ohne die ganzen Logos oder ein eigenes Branding."

- Die **Haptik** der Spielematerialien wird in der Regel als sehr wertig wahrgenommen. Insbesondere bei den Spielfeldern (Digitaldruck auf 330 gr/qm Polyester) und den Spielkarten (Digitaldruck, laminiert mit gerundeten Ecken) wird von einigen Teilnehmenden (in Führungspositionen) explizit und interessiert nach dem Material gefragt. Der Einsatz von Holz in dem LS „Informationsklassifizierung" überrascht, wird aber durchaus goutiert und als Besonderheit wahrgenommen.

7. Psychologische Grundspannungen, Typologie und Exkurs Reifegrad

7.1 Zusammenfassende Besonderheiten der Gruppendiskussionen und Fokusinterviews

Beide avisierten Zielgruppen der LS, d. h. alle Mitarbeitenden aus der finalen Anwendenden- bzw. Konsumierenden-Perspektive sowie die Awareness-Verantwortlichen und andere IT- bzw. Security-Expertinnen und -Experten als Multiplikatorinnen bzw. Multiplikatoren aus einer Art B2B-Perspektive begrüßen die getesteten Tools vehement.

Die Multiplikatorinnen und Mulltiplikatoren scheinen den Produzierenden dieser Studie das Testmaterial geradezu aus den Händen reißen zu wollen. Der Image-Wert der LS wird zwischen „Erste-Hilfe-Kasten“ und „Banner“ – in Form eines Hoheitszeichens mit Statement-Charakter für „Security-Generäle“ – verortet. Sie bemerken durch die Ausstattung eine höhere Sichtbarkeit und fühlen sich selbst mit den angebotenen Werkzeugen in Bezug auf Ihre Wirksamkeit gut für den „Ernstfall“ ausgestattet. Sie werden ernst genommen und fühlen sich geradezu beschenkt – wie folgende Zitate vermuten lassen:

„Danke dafür, das ist für mich wie Weihnachten und Ostern zugleich.“

„Wir sind darauf angewiesen, dass uns jemand einen verlängerten Arm für die Security Awareness zur Verfügung stellt. Als IT-Admin fühlt man sich oft wie amputiert, ja … beinahe hilflos. Weil uns kaum jemand zuhören mag. Auch die Kollegen nicht. Mit den Spielen schaffen wir es endlich wieder, dass uns die Kollegen sehen und zuhören.“

Auch die Anwendenden lassen sich nach Beseitigung von Unsicherheiten im ersten Zugang zunehmend in das angebotene Format und die damit verbundenen Inhalte involvieren. Security erhält dabei auch den Stellenwert eines „Socializers“, der die Menschen nach monatelanger *„Corona-Diaspora“* wieder zusammenbringt. Dem Format werden dabei die Qualitäten zugesprochen, nach denen man gerade im Kontext einer hybriden Arbeitskultur, d. h. Büro und Homeoffice im Mix, gesucht hat, um den Mitarbeitenden Begegnungsräume zu schaffen. Das Format der LS beschränkt sich eben nicht nur das Modellieren einer z. B. chilligen Kaffeehausatmosphäre, sondern bietet darüber hinaus, z. B. infolge der didaktischen Vermittlung und der moderierten Diskurse, nicht nur den Menschen, sondern auch den Organisationen einen echten Mehrwert – mithin eine Win-win-Situation.

„Das ist jetzt plötzlich, nachdem ich meine Freizeit mit TV-Nachrichten Rauf- und Runterkucken verbracht hatte, wie bei einem Lagerfeuer. Warm und schön.“

„Das könnte die Zunkunft sein – wichtige Projekte konzentriert im Homeoffice erledigen und wenn wir nicht mehr allein‘ sein wollen und ins Unternehmen fahren, passiert da was – also Programm, am besten zusammen, also in der Gruppe oder so.“

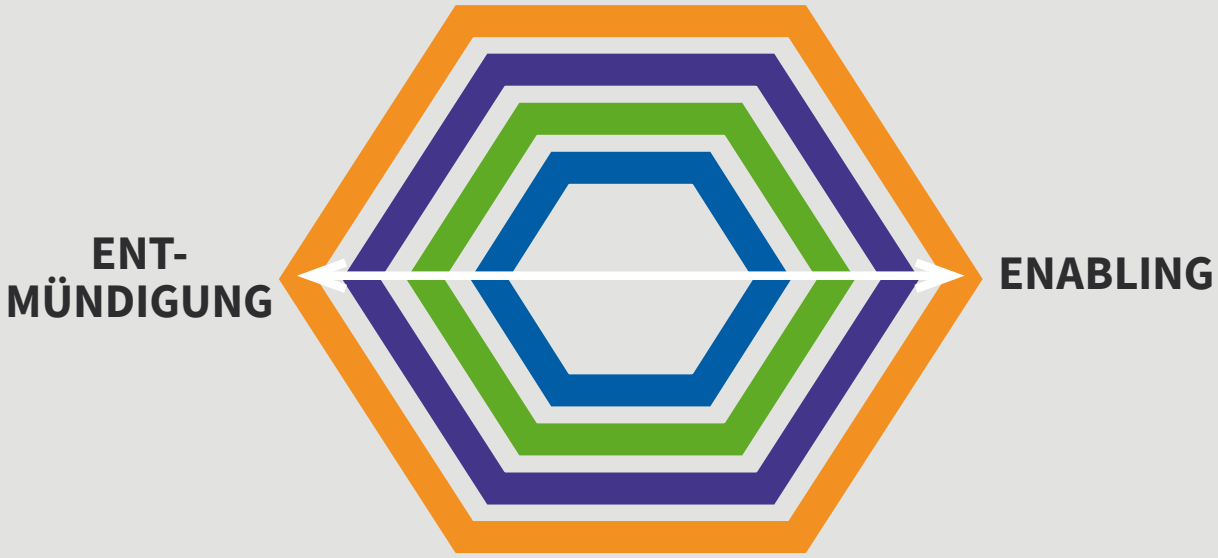
Angesichts der großen kulturellen Unterschiede in KMU funktionieren Format und Inhalte allerdings nicht überall gleich gut. Eine hybride Arbeitskultur etwa war nicht in allen untersuchten Organisationen ein Thema. Gerade die beiden in den Gruppendiskussionen nach den Spieletests befragten Unternehmen stellen zwei Extreme in der KMU-Bandbreite von Unternehmens- und Sicherheitskultur dar.

In dem einen entsteht der Eindruck, in den Spielen mit „Standard-Fällen“ konfrontiert zu werden. Diese ordnet man eher dem privaten Umfeld zu, weil man zumindest als „Normalo“, d. h. ohne exponierte Rolle in der eigenen Organisation, lediglich mit sehr redundanten Rechten ausgestattet ist. Z. B. wird darüber berichtet, dass man über keinen individuellen Internet-Zugang verfügt, was wiederum mit den verbundenen Online-Risiken wie Phishing, Ransomware, Malware begründet wird. Somit wird der eigene Arbeitsplatz als „Insel-gesteuert“ beschrieben. In Abwesenheit der Vorgesetzten wird vorsichtige Kritik an der ungewöhnlich restriktiven Sicherheitskultur des Unternehmens geäußert:

„Es fühlt sich oft unprofessionell an, keinen eigenen Internetzugang zu haben, wenn gerade keiner der Team-Plätze dafür frei ist. Es ist zum Beispiel sehr ungewohnt, auf der Arbeit im Gegensatz zum privaten Arbeitsplatz zuhause kein Online-Wörterbuch für Übersetzungen nutzen zu können.“

Über den vertiefenden Diskurs im Kontext Informationssicherheit entwickeln die Probanden/-innen eine sich mehr und mehr verdichtende Diskussion hinsichtlich Sinn und Zweck digitaler Werkzeuge mit einer zunehmend kritischen Haltung ihrer eigenen Arbeitsbedingungen, die sie im Laufe der Diskussion immer deutlicher als gefühlte Abwertung ihrer selbst benennen können. Dabei wird vor allem der Wunsch der Mitarbeitenden deutlich, im Unternehmen stärker auf das Thema Digitalisierung und Autonomie im Rahmen der eigenen Arbeitsaufgaben zu setzen.

1



2

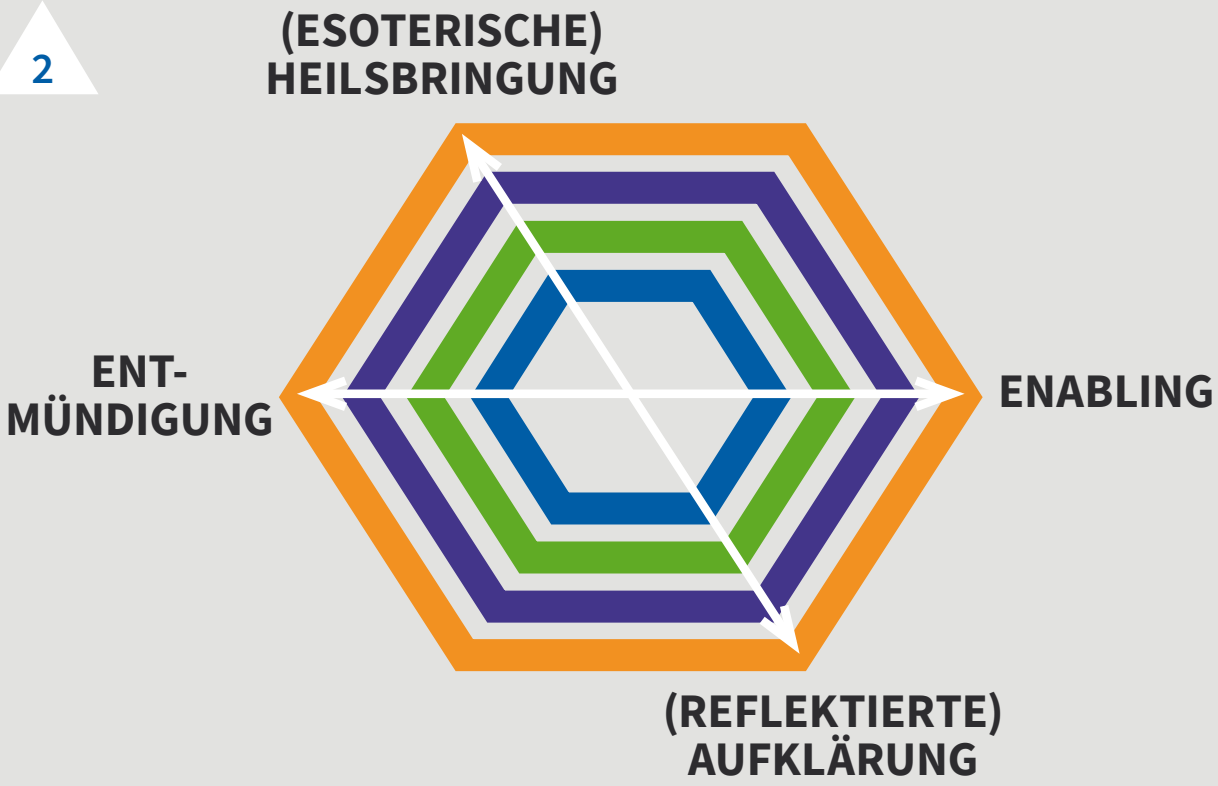


Abb. 10 und 11: *Psychologische Grundspannung Security Awareness und Nutzung von LS bzw. anderen diskursiven Tools in KMU (Teil 1 und 2 von 3)*

„Zurzeit drucken wir bestimmt Dutzende Briefe am Tag aus und versenden die per Post. Deshalb können wir auch kein Homeoffice machen."

Als unzeitgemäßer Hemmschuh wird auch die Tatsache bewertet, dass es (für die einzelnen Mitarbeitenden jeweils) nur eine E-Mail-Adresse gibt, die drei Firmierungen im eigenen Unternehmen abdeckt.

Auch das hier oft gefühlte Prinzip „Learning-by-doing", das scherzhaft, aber mit deutlicher Konnotation als „falsch Vormachen" übersetzt wird, zeigt, dass wenig Involvement im Kontext Sicherheitskultur des eigenen Arbeitgebers besteht und wenig Respekt gegenüber denjenigen, die Informationssicherheit operativ umsetzen.

Zugleich wird diese intuitiv erlebte Ebene mit offenbar kognitiv geleiteten, oft phrasenhaft zustimmenden Bekundungen angereichert, die dem anwesenden IT-Administrator sichtbar gefallen, nämlich dass das Thema Sicherheit eine immer größere Rolle im Arbeitsalltag spielt – umso mehr nach einem konkreten CEO Fraud vor zwei Wochen.

Dass auf die Frage nach den Konsequenzen dieses noch präsenten Vorfalls beinahe unisono mit dem Hinweis auf die bestehende Cyber-Versicherung verwiesen wird, demonstriert andererseits, dass wenig Sorge besteht, im Falle eines eigenen Fehlers persönliche Konsequenzen erleben zu müssen. Viel stärker wiegen in diesem Kontext Scham bzw. Kränkung ob des Vertrauensmangels durch Führungskräfte, insbesondere der Geschäftsführung. Mithilfe der Spiele werden den Mitarbeitenden hier vor allem ihre persönlichen Begrenzungen in Bezug auf Eigenverantwortung bzw. Nutzung digitaler Werkzeuge vor Augen geführt, weniger die Möglichkeiten, die Produktivität ihres Unternehmen zu erhalten, indem sie an der Seite von Führung und Sicherheitsverantwortlichen gemeinsam Informationen schützen. Die Produzierenden dieser Studie werden hierbei als offenbar lang erwartete Heilsbringer mit „Wunder-Aspergill" (liturgisches Gerät zum Besprengen mit Weihwasser) wahrgenommen, aus dem das Unternehmen wie mit Weihwasser mit Schutz, Prävention und eben Awareness als Segen besprengt werden könnte.

Beim dem anderen per Gruppendiskussion befragten Unternehmen zeigt sich eine ganz andere, deutlich selbstbewusstere Seite von Unternehmens- und Sicherheitskultur und dem Verhältnis zur Digitalisierung. Dies lässt sich unter anderem auch an Auftritt, Atmosphärischem und dem Umgang miteinander bzw. den Produzierenden dieser Studie – ganz generell an der Kommunikationskultur – festmachen Auch scheinen die Mitarbeitenden mithilfe der Spiele gedanklich in eine interessant anmutende, voller Eigenleben steckende Awareness-Welt eintreten zu können, dazu angeregt, weiter darin abzutauchen.

Dieser Sog wird deutlich über die zahlreichen, lebendigen, vertiefenden Fragen, die gegebenenfalls nicht über die Inhalte der LS abgedeckt sind, und das deutliche Strapazieren des gesetzten Zeitbudgets sowie über folgende Zitate:

„Ich habe jetzt das Gefühl, mich mit manchem beschäftigen zu müssen und zu wollen."

„Das ist wie ein Anker."

„Ich finde es so entlastend, dass es nicht um Dummheit geht."

„Man will das ja wissen. Da ist es wichtig, Hintergründe erklärt zu bekommen."

7.2 Psychologische Grundspannungen bei der Nutzung von Lernszenarien

Aus der in den Kapiteln 6 und 7.1 beschriebenen Konstellation von Unternehmens- bzw. Sicherheitskultur heraus, d. h. einerseits die Förderung digitaler Kultur mit den adäquaten Werkzeugen bei gleichzeitig belebendem Diskurs im Kontext der Informationssicherheit, andererseits restriktives Verhalten bis hin zum umfassenden Verbot einer weitgehend autonomen Online-Nutzung kann eine für KMU prototypische Grundspannung abgeleitet werden. Spürbar wird eine psychologische Konstellation, die allen seriösen Awareness-Maßnahmen inhärent ist und bei der sich eine psychologische Gestalt im Sinne eines produktiven Veränderungsprozesses in Verwandlung begibt.

Diese Grundspannung konnte nicht nur anhand der Gruppendiskussionen evaluiert werden, sondern auch während des mühevollen Akquiseprozesses und abgeleitet aus den 20 Jahre Beratungserfahrung der Produzierenden mit Awareness-Maßnahmen – auch in KMU.

Am besten beschreibbar ist sie durch die Phrase...

(digitales) Enabling
vs. Entmündigung.

Die vorliegende Konstellation gibt darüber hinaus Aufschluss über die Beziehung der Sicherheitskultur zum Thema Security Awareness in Form einer Grundspannung ...

(reflektierte) Aufklärung
(Awareness als reifes Managen von Informationssicherheitsrisiken und Übersetzen von Veränderungsprozessen im Kontext der Digitalisierung)

vs.
(esoterische) Heilsbringung
(Awareness als Wunschkonzert u. a. zur Angst-Reduktion im Umgang mit Risiken)

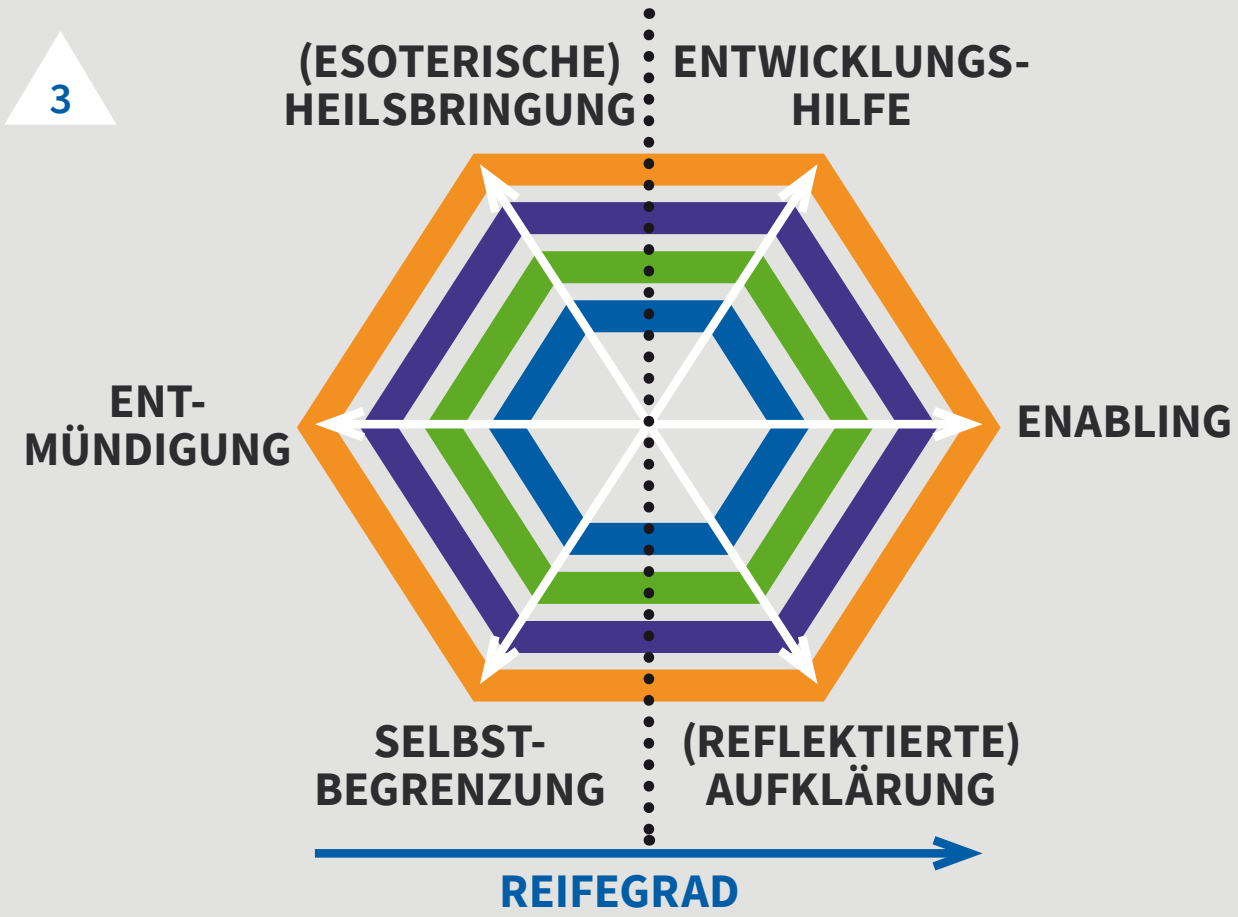


Abb. 12: *Psychologische Grundspannung Security Awareness und Nutzung von LS bzw. anderen diskursiven Tools in KMU (Teil 3 von 3)*

Schließlich kann als dritte Grundspannung in Bezug auf den konkreten Umgang mit den LS als Awareness-Tool eine Konstellation …

Entwicklungshilfe

(Lernstationen als diskursives Format im Sinne einer psychologischen Verwandlungsintention).

vs.

Selbstbegrenzung

(Lernstationen als Spiegel auferlegter Beschränkung der Mitarbeitenden durch die Organisationskultur)

… abgeleitet werden.

Gleichsam ergibt sich aus der Anordnung dieser drei Konstellationen in diesem als Grundform gewählten Sechseck (s. Abb. links) ein Modell für den Reifegrad im Kontext Security Awareness (s. Kapitel 7.3).

Das heißt: Innerhalb einer Organisation, die beinahe ausschließlich auf Abdichten statt Öffnen setzt und Mitarbeitende mit einer eher regressiven Kultur von Verboten und Verschließen begegnet, kann Security Awareness wenig ausrichten. Denn die motivatorische Grundlage von Sensibilisierung nährt sich unter anderem aus dem Thrill eines Risikos. D. h. dort, wo Risikovermeidung gelebt wird, kann der Aufruf zur Prävention, zu sicherem Verhalten keine Echoräume finden, um den Benefit von Sensibilisierung z. B. in Form von Autonomie zu atmen, Risikokultur bewusst und selbstbestimmt zu leben.

Awareness ohne Anwendungsräume verpufft daher in ein Nichts, weil keine lebendige Bühne zur Weiterentwicklung bereitgestellt wird. Daraus ergibt sich das Paradox, dass gerade dort, wo die Awareness-LS vermeintlich am dringendsten gebraucht werden, der fehlende Mindestumsatz in Bezug auf eine Absicht mehr oder weniger unbewusst boykottiert wird. Und dort, wo ein offener Umgang mit Kommunikationskultur und Digitalisierung besteht, ein schon erhöhter Security-Reifegrad noch weiter gesteigert werden kann.

Auf diesen wichtigen Aspekt wurde bereits in der 2006 produzierten Studie über Fehlerkultur „Entsicherung am Arbeitsplatz“ [6] in aller Breite hingewiesen. *„Security soll Identifikationsinhalte schaffen. Es fällt auf, dass es bei den Testpersonen (…) ein größeres Interesse an direkten Auseinandersetzungen (z. B. Duellieren) (…) gibt: Im Sinne einer Belebung und Dramatisierung entmenschlichter Arbeitsverfassungen lässt sich dieses Bild auch als ‚Abwehr‘ bzw. ‚Kampf‘ aufgreifen (…) es geht (…) um ein sinnliches Einbeziehen der Mitarbeiter. Das Einbeziehen funktioniert aber nur vor dem Hintergrund einer lebendig-spannenden Security mit Identifikationspotenzial.“* [6] (s. dort S. 54-55).

7. 3 Exkurs Security Awareness-Reifegrad und -Messungen

Im Bereich von Forschung und Anwendung existieren bisher relativ wenige Ansätze in Bezug auf einen Security Awareness-Reifegrad. Bei vorhandenen Modellen werden verschiedene, oftmals nur rudimentär definierte Ausprägungen von Wissen, Kommunikationskultur, Strategie und quantitativen Evaluationen miteinander kombiniert. Diese Kombinationen zielen im Wesentlichen auf die Intention eines sicherheitskonformen Verhaltens ab.

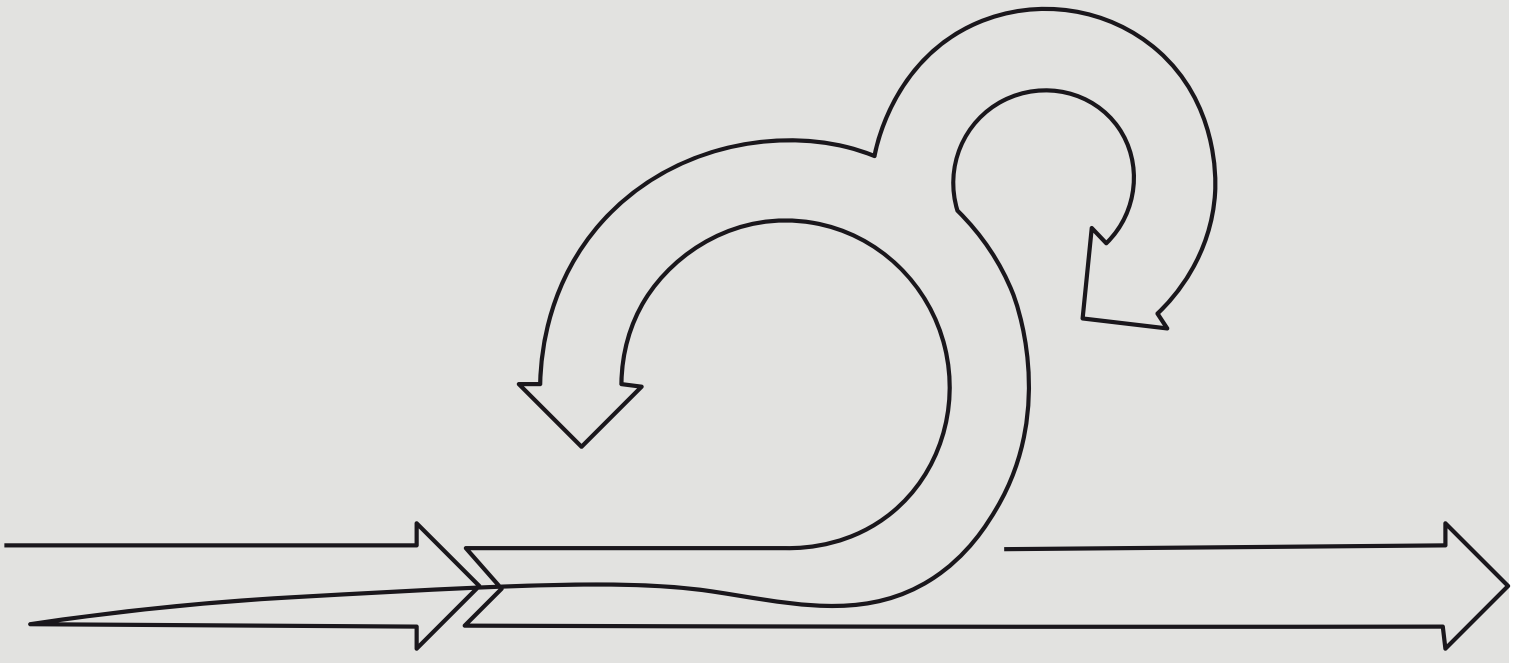
Eine entsprechende Entwicklung einer lebendigen, aktiv modellierten Sicherheitskultur, die auch Erfahrungen oder Entwicklungsperioden beinhaltet, korrespondiert in den meisten Modellen mit einem höheren Reifegrad.

Als Beispiele werden nachfolgend einige der Reifegrad-Modelle ohne Anspruch auf Vollständigkeit vorgestellt.

7.3.1 KnowBe4: Security Culture Maturity

Der Security Awareness-Plattform-Anbieter KnowBe4 hat mit dem so genannten „Security Culture Maturity“-Modell laut begleitendem Marketing-Text 2022 das potenziell *„erste Reifegradmodell der Branche“* [7] entwickelt, eine Aussage, die in dieser Form nachweislich nicht haltbar ist. Hierbei wird der Reifegrad mehr oder weniger mit so genannter „Security-Culture“ gleichgesetzt, d. h. es handelt sich im Wesentlichen um eine Balanced Score Card, innerhalb der Security Awareness-Faktoren auf bis zu fünf verschiedenen Ebenen einer Sicherheitskulturmatrix mit einem Gesamtpunktehöchstwert von maximal 100 festgeschrieben sind, eine Matrix, die neben Awareness auf einer Vielzahl von weiteren sicherheitsrelevanten Faktoren basiert:

- **Level 1 – Basic Compliance:** Minimum an Training, begrenzte quantitative Metriken
- **Level 2 – Security-Awareness-Foundation:** mindestens ein jährliches Training und Onboarding-Schulungen, gelegentliche Phishing-Simulationen, inhaltliche Vielfalt
- **Level 3 – Programmatic-Security-Awareness & Behavior:** strategisches Sensibilisierungsprogramm mit integrierten Tools, vierteljährliches Training mit simuliertem Phishing, Intention eines sicherheitsbewussten Verhaltens
- **Level 4: –Security-Behavior-Management:** kontinuierliche Schulungen über verschiedene Kanäle und für unterschiedliche Zielgruppen, verstärkter Einsatz integrierter Tools zur Kommunikation der Trainingsstrategie, Intention einer „echten“ Verhaltensänderung
- **Level 5 – Sustainable Security Culture:** Programm, das die Sicherheitskultur bewusst misst, formt und stärkt, unterschiedliche Methoden eines verhaltensbasierten „Encouragement“, KPIs die die Organisationskultur ganzheitlich betreffen [7]



7.3.2 SANS Institute: Security Awareness Maturity Model

Einen ähnlichen Ansatz verfolgt seit 2011 ein weiterer großer Player unter den Security Awareness-Dienstleistenden, das SANS Institute, unter dem Titel „Security Awareness Maturity Model“ [8]:

- **Level 1 – Nonexistent:** Ein Awareness-Programm existiert nicht, Mitarbeitenden ist nicht bewusst, dass sie ein Angriffsziel darstellen und ihr Verhalten direkte Auswirkungen auf die Sicherheit des Unternehmens ausübt, sie kennen oder befolgen die Unternehmensrichtlinien nicht,sind leichte Angriffsopfer
- **Level 2 – Compliance Focused:** Pragmatische Awareness, um Compliance- oder Audit-Anforderungen zu erfüllen, Trainings werden anlassbezogen angeboten – beschränkt auf jährliche Events, Mitarbeitende haben kein oder kaum Bewusstsein in Bezug auf Unternehmensrichtlinien und/oder ihrer Rolle beim Informationsschutz
- **Level 3 – Promoting Awareness & Behavior Change:** Ausdifferenzierung von Zielgruppen und Themen mit größtem Impact, über jährliche Pflichtveranstaltungen hinaus wird kontinuierliche Verstärkung.angeboten, Inhalte werden auf ansprechende, positive Weise kommuniziert, die zu Verhaltensänderungen anregen soll, Mitarbeitende verstehen und befolgen Richtlinien, erkennen bzw. melden Vorfälle, die sie auch zu verhindern versuchen
- **Level 4: – Long-Term Sustainment & Culture Change:** Umfasst Prozesse, Ressourcen und explizit Management Attention, um einen langfristigen Awareness-Lebenszyklus zu gewährleisten, berücksichtigt mindestens eine jährliche Überprüfung, Awareness-Content ist aktuell, ansprechend und etablierter Bestandteil von Sicherheitskultur, umfasst außerdem einen Change in Bezug auf Verhalten, Überzeugungen, Einstellungen, Wahrnehmungen
- **Level 5 – Metrics Framework:** Ausgereiftes Programm mit einem robusten Metrik-Rahmenwerk für jede einzelne Phase, daher kontinuierliche Verbesserung mit dem Nachweis eines Return on Investment als Mehrwert [8]

Abgesehen von den erklärungsbedürftigen Unterscheidungen zwischen „echten“ und der somit inhärenten Logik nach „unechten“ Verhaltensänderungen, sind die beiden letzten Ansätze zur Darstellung eines Security Awareness-Reifegrads weitgehend ungeeignet, da die Sensibilisierung beider Anbietenden beinahe ausschließlich auf Training, mithin Lerntheorie, abzielt und weitere Faktoren wie Marketing, Psychologie bzw. systemische Kommunikation nicht oder kaum berücksichtigt werden.

7.3.3 TreeSolution: Capabilty Maturity Model und Security Awareness Radar

Der Schweizer Gründer und Inhaber des Security Awareness-Dienstleisters TreeSolution, Dr. Thomas Schlienger, hat mit dem CMM (Capabilty Maturity Model) [9] ein Reifegradmodell entwickelt und zum Ziel-Framework seiner quantitativen Messmethode „Security Awareness Radar“ [10] erhoben, das stark an das oben erwähnte Modell des SANS Institute erinnert. Hierbei unterscheidet er – von unten nach oben – fünf Stufen:

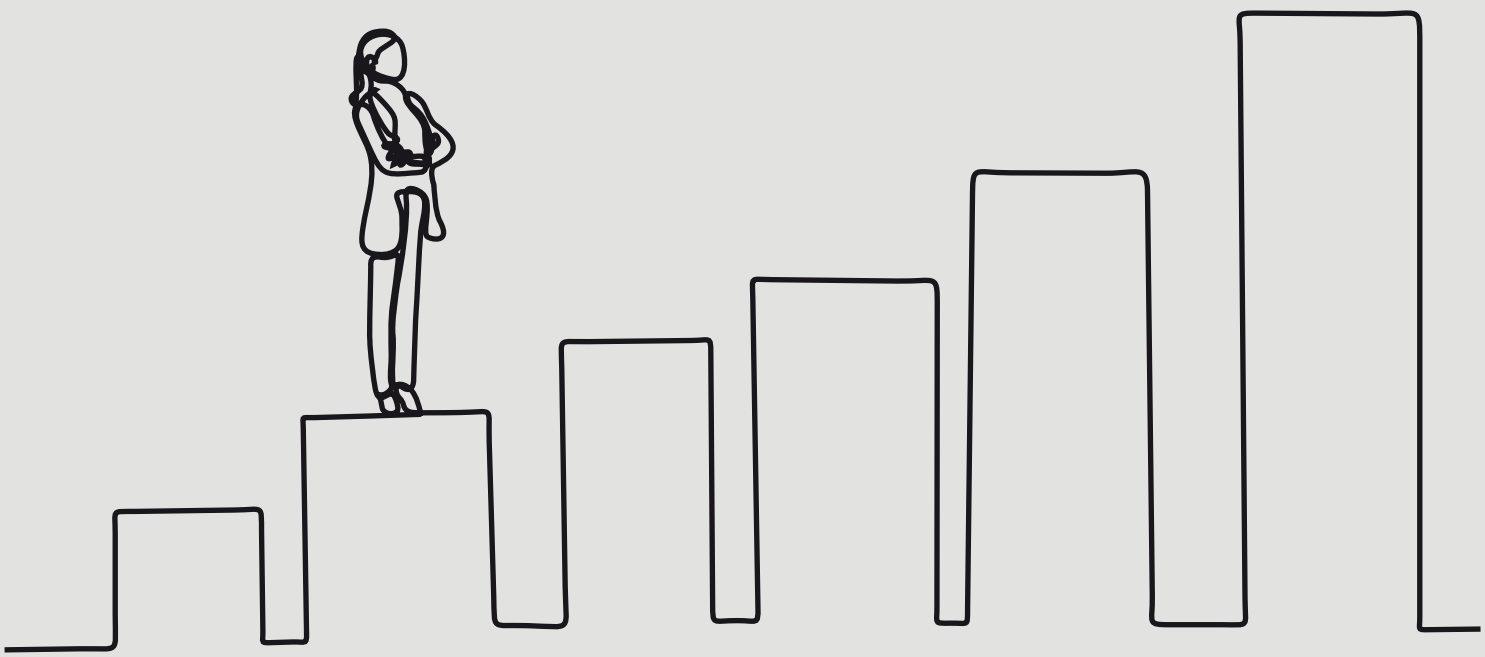
- **Beginnend:** Kein Awareness-Programm
- **Wiederholbar:** Compliance fokussiert
- **Definiert:** Fördert Bewusstsein und Veränderung
- **Gesteuert:** Langfristige Perspektive
- **Optimierend:** Mess-Rahmenwerk

Das Tool misst im Rahmen eines so genannten „Informationssicherheits-ABC“ Awareness, Behaviour, Culture, „starke“ und „schwache Punkte“ in den Bereichen Bewusstsein, Verhalten und Kultur [10]. Laut Schlienger muss das Ziel die Entwicklung eines robusten Mess-Frameworks sein, das *„erlaubt, die Entwicklung und Wirkung Ihrer Awareness-Maßnahmen aufzuzeigen.“ Außerdem: „Die langfristige und kontinuierliche Weiterentwicklung der Maßnahmen“ und die „Verankerung in der Unternehmenskultur“* [9].

Fragen zu den einzelnen Stufen, die sich unter anderem vor allem im Kontext der Terminologie bzw. einer empirischen Stützung ergeben:

- **Beginnend:** Womit beginnend? Ausgehend vom ersten Axiom der Kommunikationstheorie eines Paul Watzlawick, „Man kann nicht nicht kommunizieren“ [11], existiert auch keine Organisation ohne Sicherheitskommunikation bzw. Awareness.
- **Wiederholbar:** Sind die anderen Stufen nicht (per se auch) „Compliance fokussiert“?
- **Definiert:** Fördern die anderen Stufen nicht „Bewusstsein und Veränderung“? Wenn ja, wie wären diese im Kontext Awareness einzuordnen, wenn das Kernziel von Awareness stets eine Bewusstseinsveränderung zum Ziel hätte?
- **Gesteuert:** Wie lässt sich eine „langfristige Perspektive“ steuern, wenn Zukunft generell als immer weniger vorhersehbar betrachtet wird?
- **Optimierend:** Welche empirische Grundlage existiert hinsichtlich der These, dass der Awareness-Reifegrad durch ein „Mess-Rahmenwerk“ auf die höchste Stufe gehoben wird?

Aus Sicht dieser Evaluation kann hinsichtlich dem „Markenkern“ von Security Awareness – die Intention, das Bewusstsein der Mitarbeitenden im Umgang mit sicherheitsrelevanten Tätigkeiten zu stärken – auch kein Mehrwert infolge einer quantitativen Betrachtung von Maßnahmen identifiziert werden. Gleichwohl schafft eine Messung Auf-



merksamkeit für die Belange der Informationssicherheit. Wenn versucht wird, ein Thema zu bemessen, es in Zahlen auszudrücken, zahlt allein der Prozess der Fragebögen-Implementierung oder die Veröffentlichung der evaluierten Key Performance Indicators (KPIs) auf das Image der Informationssicherheit ein. KPIs sind zwar kein primäres Awareness-Instrument, sensibilisieren jedoch mindestens das Management einer Organisation auf einer Awareness-Metaebene, nämlich vor allem in Bezug auf bereit zu stellende Security Awareness-Budgets und idealerweise hinsichtlich einer Positionierung der eigenen Organisation im Umfeld vergleichbarer Unternehmen mithilfe von Benchmarks. Eine Koppelung mit einem höheren Awareness-Reifegrad ist jedoch nicht unmittelbar nachweisbar.

7.3.4 Prof. Konrad Zerr: SAI – Security Awareness Index

Im deutschsprachigen Bereich existiert neben dem „Security Awareness Radar" von TreeSolution eine weitere Messmethode hinsichtlich Security Awareness, die wie das TreeSolution-Tool z. B. Branchen-Benchmarks auf Basis von KPIs erlaubt, die mithilfe eines standardisierten Fragebogens evaluiert werden. Entwickelt wurde dieses Messkonzept von Prof. Konrad Zerr von der Hochschule Pforzheim. *„Ausgangspunkt ist immer eine ausführliche Bestandsanalyse"* [12]. Analysiert werden *„implementierte Security Awareness-Maßnahmen, Organisationsstruktur, vorhandene Sicherheitsregelungen, Sicherheitskultur"* [12]. Auf Grundlage der grundsätzlichen Zielsetzung der Security-Policy und der durchzuführenden Messung des Sicherheitsbewusstseins wird *„ein Erhebungskonzept entwickelt. Dieses definiert die zu beantwortenden zentralen Fragen, die zu betrachtenden Organisationseinheiten und die einzusetzenden Erhebungsinstrumente. Das Erhebungskonzept wird (…) im Rahmen von Expertengesprächen validiert und geht danach in die operative Umsetzung. Am Ende stehen die Auswertung und Interpretation der gewonnenen Einsichten und die Ableitung von Handlungsempfehlungen. Ein zentraler Bestandteil des Erhebungskonzepts ist meist ein teilstandardisierter Fragebogen, der neben offenen Antwortmöglichkeiten auch die Ableitung standardisierter Kennziffern (SAI – Security Awareness Index) in einer unternehmensrepräsentativen Weise ermöglicht. Dieser besteht aus teils standardisierten, teils kundenindividuell entwickelten Fragestellungen. Die standardisierten Fragen sind deduktiv, d.h. theoriegeleitet entwickelt und im Rahmen mehrerer Praxis-Projekte auf ihre Reliabilität hin überprüft. Die individuellen Fragen werden spezifisch und kontextbezogen mittels Expertengesprächen entwickelt"* [12]. Die Dimensionen, die zur Ermittlung des SAI herangezogen werden, sind u. a. „Verantwortlichkeit", „Einfluss auf Aufgabenbewältigung", „Unternehmenskultur", „Management Attention" oder „Einstellung zur Sicherheit."

Ausgehend von den Ergebnissen der Gruppendiskussionen im Kontext der hiesigen Evaluation und den diversen von known_sense produzierten Vorgängerstudien – vor allem „Bluff me if u can" [13] – erscheint Insbesondere die Dimension „Management Attention" geeignet, den Reifegrad zu beeinflussen. Gemeint ist damit die Aufmerksamkeit von Führungskräften in Bezug auf Sicherheitsthemen, vor allem aber auch die Unterstützung der Mitarbeitenden infolge der Vorbildfunktion des Managements. Allerdings muss angezweifelt werden, dass eine derartige Dimension sich allein aus subjektiven Zustimmungen auf Fragebogen-gestützte Thesen wie „Meine direkte Führungskraft diskutiert mit uns regelmäßig über Sicherheitsthemen" vergleichbar aufrechnen lässt.

7.3.5 Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt

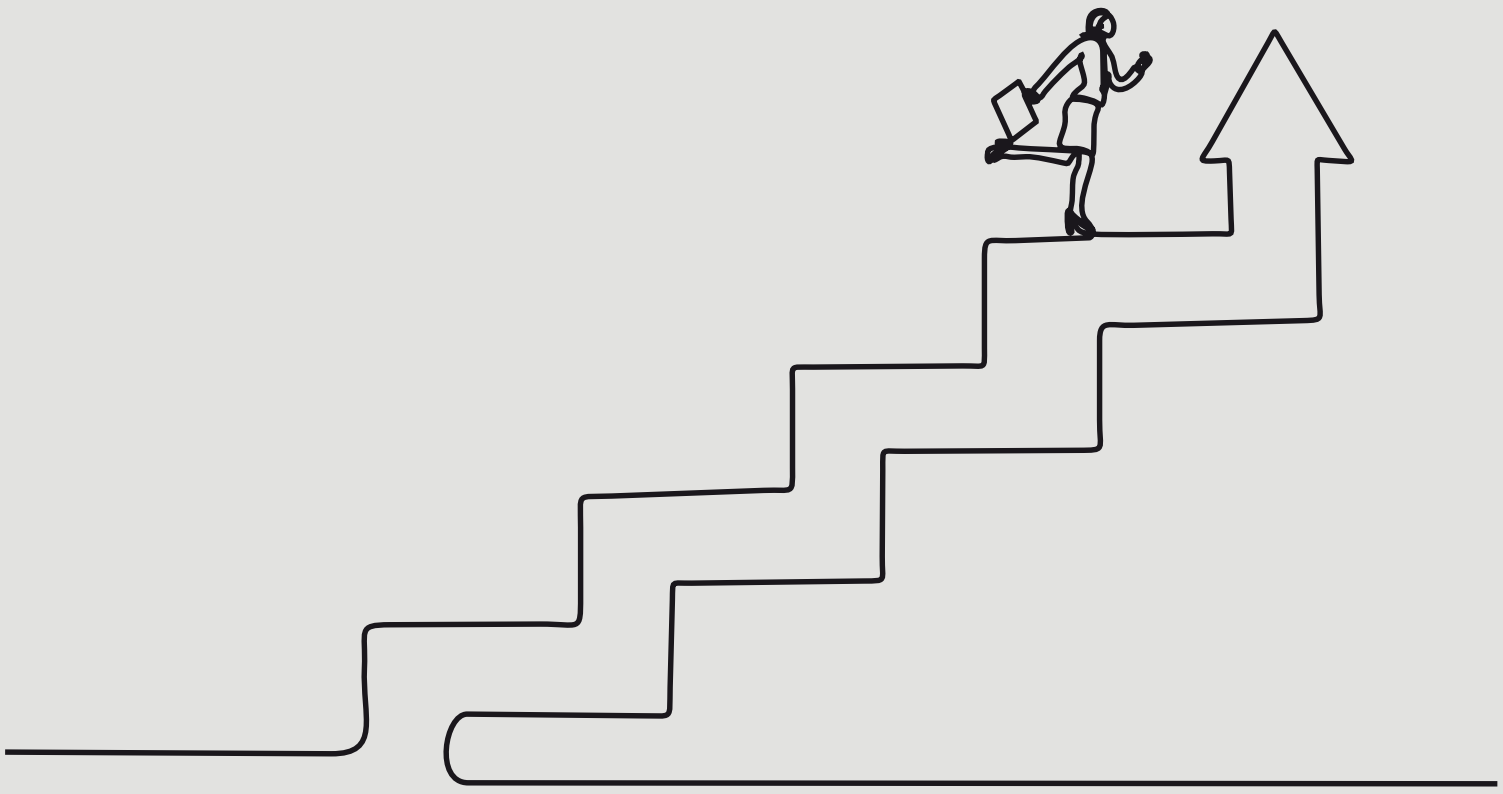
An einem abweichenden, allerdings zum Zeitpunkt der hiesigen Studienerstellung noch unveröffentlichten Reifegrad-Modell, das jedoch auch die Intention eines sicherheitskonformen Verhaltens berücksichtigt, forscht aktuell die Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt. Security Awareness wird dort, basierend auf dem integrierten Verhaltensmodell von Montano and Kasprzyk [14] als Gesamtheit aus „Wissen und Fähigkeiten", „Verhaltensabsicht", „Salienz" und „Gewohnheit" definiert, deren Zusammenspiel in der Absicht, ein sicherheitskonformes Verhalten anzustreben, durch so genannte „Einschränkungen aus dem Umfeld" gestört wird.

Tiefenpsychologisch könnte man hinter der Hilfskonstruktion „Einschränkungen aus dem Umfeld" als eine Entsachlichung kognitiver und rationaler Absichten ein „menschliches Eröffnen" vermuten, d. h. so genannte „Fehlleistungen" wie sie typisch sind für die paradoxen Verhältnisse, die entstehen, wenn Informationssicherheit die Schaffung eines komplett abgedichteten Schutzraums anstrebt, der jedoch bei konsequenter Zuspitzung alles Menschliche, alles Lebendige im Keim erstickt und abtötet und unbewusste Reaktionen bei den Handelnden, den Menschen, provoziert, in aller Breite dargestellt in der Studie „Entsicherung am Arbeitsplatz". [6]

Hinsichtlich der Methodik, eine Diskrepanz („abstraktes Delta") zwischen dem Wunsch und dem Ist-Zustand berechnen zu wollen, bedient man sich hier dem so genannten „Rasch Modell" [15], eine Maximum-Likelihood-Methode, entwickelt vom dänischen Statistiker Georg Rasch, u. a. im Einsatz bei der Bewertung von Probanden/-innen im Rahmen der PISA Studien:

- Hoher IST + Niedriger Wunsch = **eher sehr leichtes Item**
- Hoher IST + Hoher Wunsch = **eher leichtes Item**
- Niedriger IST + Hoher Wunsch = **eher schweres Item**
- Niedriger IST + Niedriger Wunsch = **unnötiges Item**

Auch hier wird „Messung" neben „Förderung", „Prozesse" sowie „Organisation und Management" als eine Item-



Gruppe zur Berechnung für insgesamt fünf Levels herangezogen.

„Anschließend werden alle Items nach Schwierigkeit sortiert, Infit sowie Outfit geprüft, mithilfe von SPSS (Statistical Package für Social Sciences) in jeweils eigenem Cluster geclustert und über die Differenzen der Schwierigkeiten in Levels zusammengefasst“ [16].

Dass hier ein so genannter Awareness-„Wunsch“, gemeint sind vermutlich unter anderem Intention, Absicht, Purpose, berücksichtigt wird, unterscheidet das Modell von den anderen, hier dargestellten erheblich und entspricht auch den hiesigen Beobachtungen, Interviews und Gruppendiskussionen, insbesondere hinsichtlich eines möglichen (unbewussten) Boykotts von produktiver bzw. proaktiver Entwicklung von Sicherheitskultur durch eine Begrenzung der Beschäftigten-Autonomie, z. B. am digitalen Alltag teilzuhaben.

7.3.6 Reifegrad auf Basis des known_sense-Layer-Modells

Ausgehend von den bisher bekannten und zum Teil oben beschriebenen Ansätzen und dem Layer-Modell von known_sense, dargestellt u. a. in der KMU-Grundlagenstudie [2] auf S. 15, und basierend auf der hiesigen Evaluation, kann für KMU im Folgenden ein vereinfachtes Positionierungs-Modell 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. Dieses Modell berücksichtigt auch die Intention eines Enabling von Mitarbeitenden hinsichtlich digitaler Werkzeuge im Sinne einer Botschaft wie „Nutze jede technische Innovation, die dir nützt, aber bitte sicher“:

- **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. reinen Wissensvermittlung (z. B. Layer 1: Lerntheorie – s. Grundlagenstudie [2], S. 14).
- **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 – s. Grundlagenstudie [2], S. 14).
- **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 – s. Grundlagenstudie [2], S. 14).

Aus dem Ranking ergeben sich unter anderem folgende Aufgaben hinsichtlich einer produktiven Implementierung von Security Awareness und insbesondere Awareness-LS:

- **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, LS inklusive.
- **Awareness-Reifegrad = 1:** Die Organisation verfügt über keine Sensibilisierungserfahrung – bei einer beabsichtigten Nutzung ist auf LS 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 LS 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 LS 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 LS, auch mit hoher Komplexität, steht nichts im Weg.

Das oben beschriebene Modell, das den Security Awareness Reifegrad anhand integrierter Methoden (Lerntheorie, Marketing, systemische Kommunikation) und daraus abgeleiteter Kommunikationsansätze (Kanäle, Medien, Tools) herleitet, korrespondiert auch mit der psychologischen Konstruktion der Positionierungsmatrix aus Kapitel 7.2. Entmündigung mit der Begrenzung digitaler Werkzeuge im Rahmen des Arbeitsprozesses und einer mehr oder minder quasi-esoterischen Perspektive auf das Thema Awareness steht dabei für einen eher geringen Reifegrad,

**In Kleinst- (bis 9 Mitarbeitende) bzw. Kleinunternehmen (bis 50 Mitarbeitende) kann auf die Berücksichtigung des Layer 2 verzichtet werden, da Awareness-Marketing-Instrumente stets Stellvertretende für die IT- bzw. Security-Professionals darstellen. Diese Stellvertretendelogik macht ausschließlich Sinn ab einer bestimmten Größenordnung von etwa 50 oder noch mehr Mitarbeitenden. Darunter sind z. B. Face-to-Face-Dialoge erfolgreicher und direkter als das Buhlen um Aufmerksamkeit mithilfe klassischer Marketing-Werkzeuge.*

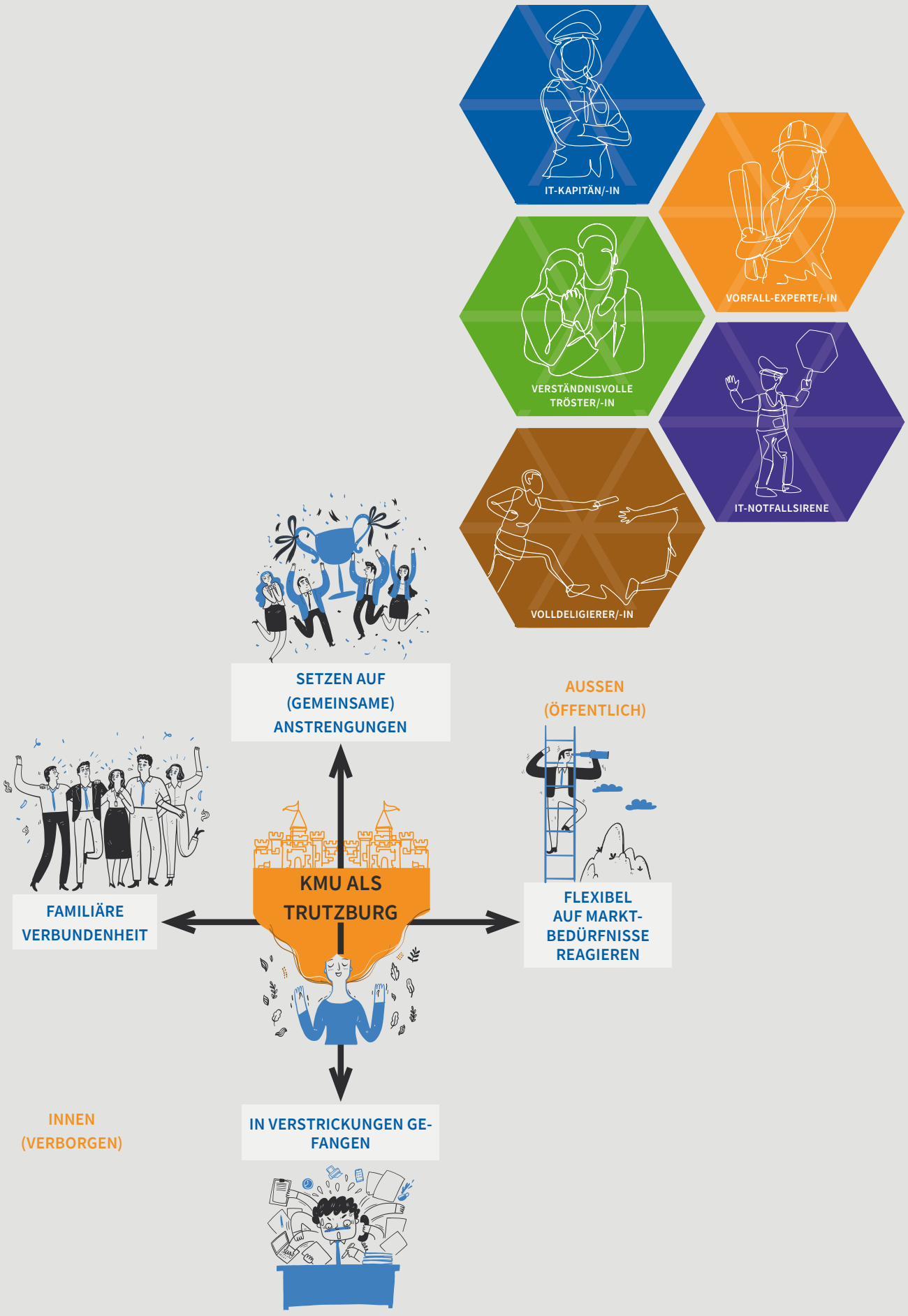


Abb. 13 und 14: *Psychologische Konstruktion der Sicherheitskultur in KMU (oben rechts) und Typologie Security-Multiplikatorinnen und Multiplikatoren (unten links) aus der KMU-Grundlagenstudie*

der sich durch Unterstützung der Mitarbeitenden in Bezug auf Digitalisierung und einer selbstbestimmten, gemanagten, aufklärerischen Sichtweise in Bezug auf Security Awareness deutlich steigern ließe.

Die hier vorgestellten Modelle sind jeweils als eine Option unter vielen möglichen Ansätzen zu betrachten. Die Disziplinen Informationssicherheit und Security Awareness verfügen über zahlreiche Einstiege zur Definition bzw. Bewertung von KPIs, die am Ende als eine ganzheitlich designte Balanced Scorecard Reifegrad oder Sicherheitskultur bemessen und darstellen. Sämtliche quantitative Ansätze müssen jedoch am Ende auf Wirksamkeit und andere Faktoren hin interpretiert und in zielführende Maßnahmen übersetzt werden.

7.4 Passung zur psychologischen Konstruktion von Sicherheitskultur und Typologie von Vorgängerstudien

Die in der KMU-Grundlagenstudie [2] auf den S. 32–33 evaluierte psychologische Konstruktion von Sicherheitskultur in KMU mit der Kehrseite so genannter „gemeinsamer Anstrengungen" in Form von „Verstrickungen" konnte mithilfe des hiesigen Tests weitgehend bestätigt werden.

- Nichtbeachten von Regeln mit damit verbundenen Security Incidents führt selten zu Konsequenzen – im Worst Case wird die Cyberversicherung bemüht.
- Dies führt jedoch nicht überall zu Unmut in der IT-Administration, manche fühlen sich in ihrer Position durch eine externe Delegation im Schadensfall z. B. an eine Versicherung offenbar deutlich sicherer als mit der internen Delegation von Schutzmaßnahmen an Kolleginnen und Kollegen – zu Lasten der Durchsetzung nachhaltiger Security Awareness.
- Durch die Auseinandersetzung mit den LS Themen im Rahmen des Tests wird den Probanden/-innen bewusst, dass die bisherigen Maßnahmen im Unternehmen gegebenenfalls nicht ausreichen (bewusste Inkompetenz) oder sogar, dass sie sich generell in einem digitalen Autonomie-Dilemma befinden und wenig Verantwortung übertragen bekommen.
- Die zuvor als positives Merkmal hervorgehobenen eigenen Anstrengungen zeigen sich in den Gruppendiskussionen angesichts der immer stärker in den Blick genommenen Gefahren als individuelle Überforderungen oder verunsicherte Maßlosigkeit, etwa indem man die avisierte Spielzeit bei den getesteten LS um das Dreifache überschreitet und am liebsten gar nicht mehr aufhören will, über die (neu erlernten) Risiken zu sprechen – auch nicht im Rahmen einer „Zugabe" in Form eines gemeinsames Mittagessens.

Die in der Grundlagenstudie [2] auf den Seiten 36 bis 37 evaluierte psychologische Typologie im Mix der befragten Geschäftsführernden, Security-Professionals und deren Multiplikatorinnen bzw. Multiplikatoren, …

- IT-Kapitän/-in,
- Vorfall-Experte/Expertin,
- Verständnisvolle Tröster/-in,
- IT-Notfallsirene,
- Volldelegierer/-in

… konnte mithilfe des hiesigen Tests ebenfalls bestätigt werden. In den Gruppen dominierten allerdings vor allem Umgangsformen, die auf eine/n „IT-Kapitän/-in" oder den bzw. die „verständnisvolle Tröster/-in" hinweisen. Dies kann auf eine gewisse Färbung bei dem internen Selektionsprozess im Rahmen der Auswahl von Teilnehmenden durch die Organisationen selbst zurückgeführt werden.

Es konnte aber auch eine Passung zur Typologie der von known_sense und Partnern produzierten Wirkungsanalyse zum Thema „Selbstbild von Security-Professionals", „Aus dem Abwehr in den Beichtstuhl" [17] evaluiert werden.

In der Ausübung einer Tätigkeit als Expertin oder Experte im Informationssicherheitsbereich sind zum Teil unbewusste Aktionen bzw. Reaktionen enthalten, die zu einer Lösung der schwierigen, paradoxen Grundprobleme der Security im Zusammenspiel von Strategien, Wirkungen und Image führen sollen. Die sozialen und kommunikativen Strategien der hier befragten Awareness-Verantwortlichen und deren Multiplikatorinnen bzw. Multiplikatoren können wechselseitig auf drei Prototypen verteilt werden:

- Die bzw. der „General/-in"
- Die bzw. der „Sicherheitswellnessbeauftragte"
- Die bzw. der „Awareness-Amputierte"

Sämtliche Typen existieren nicht in der hier dargestellten Reinform. Vielmehr ist die Tätigkeit im Sicherheitsbereich wie auch andere durch eine Konstellation verschiedener typischer Phänomene bestimmt. Man kann also die Typen – je nach Situation bzw. psychologischer Verfassung – als die verschiedenen Gesichter einer Security-Expertin bzw. eines Security-Experten verstehen.

Die bzw. die „Genral/-in" will am liebsten klare Verhältnisse und führt einen unternehmensinternen Kleinkrieg gegen alles, was sich ihrer bzw. seiner Vision einer 95%igen Sicherheit entgegenstellt – manchmal auch gegen die eigenen Kolleginnen und Kollegen. Sicherheitslücken werden mithilfe ihrer bzw. seiner Wirkmacht und *„harten Badagen"* – so gut es geht – einfach *„beseitigt"*. Die umgesetzten Sicherheitsmaßnahmen sind eher restriktiv; Awareness-Maßnahmen sind für sie bzw. ihne wie *„Weihnachtskugeln am Tannenbaum"* – sie werden mehr oder weniger aus Imagegründen als schmückendes Beiwerk ihrer bzw. seiner multiplen *„Luft- und Bodenoffensiven"* schlichtweg

Abb. 15: *Typologie Security-Professionals bzw. Awareness-Verantwortliche 2022 (links) im Vergleich zur Studie 2008 (rechts)*

ausgestellt und ansonsten nur dann goutiert, wenn sie *nachweislich* (rein quantitativ) eine hohe Wirksamkeit belegen. Klare Verhältnisse und Respekt sind ihr bzw. ihm wichtiger als der persönliche Austausch. Allzu vertiefende Diskurse sind dabei eher störend. Es ist vielmehr die Ebene der lerntheoretischen Wissensvermittlung der LS, und die Bühne einer großen „Arena" hinsichtkich der eigenen perfomeance die ihn/ihr primär interessieren.

Mit diesem Bild entspricht sie bzw. er am ehesten dem Typus „Zentrale Kontrollinstanz" oder „Fräulein Rottenmeier" aus der Studie „Aus dem Abwehr in den Beichtstuhl" [17] (s. dort S. 24-28).

Die bzw. der „Sicherheitswellnessbeauftragte" versteht sich primär als Vertretende/-r interner Dienstleistungen. Für sie bzw. ihn ist es wichtig, dass sich die Kolleginnen und Kollegen mit dem Thema Informationssicherheit wohl fühlen. Sie bzw. er braucht Security Incidents, um in der Rolle als Helfende oder Helfender agieren zu können. Daher goutiert sie bzw. er jede Awareness-Maßnahme, die ihr oder ihm als Beschleuniger ihrer bzw. seiner Ansprüche zur Verfügung gestellt wird – diese sollen jedoch vor allem die soziale bzw. kommunikative Qualität am Arbeitsplatz verbessern, damit hier eine wärmende Lagerfeueratmosphäre entsteht. Denn sie bzw. er geht davon aus, dass diese auch positiv auf die gesamte Sicherheitskultur abfärbt und damit die Anzahl an Vorfällen zu reduzieren hilft. Eine Kehrseite ist der damit verbundene „Goldene Käfig", d. h. würde sich infolge von Security Awareness eine allzu hohe Security-Kompetenz der Mitarbeitenden entwickeln, könnte diese gegebenenfalls ihre bzw. seine positiv aufgeladene Rolle in der Organisation kannibalisieren.

Mit diesem Bild entspricht sie bzw. er am ehesten dem Typus „Sicherheitsservice" oder „Mutter Teresa" aus der Studie „Aus dem Abwehr in den Beichtstuhl" [17] (s. dort S. 29-33).

Die bzw. der „Awareness-Amputierte" sucht vor allem den Kontakt mit den Kolleginnen und Kollegen, um den für sie bzw. ihn wichtigen Austausch zu fördern, leidet aber an den eigenen hohen Ansprüchen. Denn zunehmende Bedrohungen mit einer hohen Aus- und Belastung verhindern, dass ihr bzw. ihm ausreichend Ressourcen – vor allem hinsichtlich Awareness – zur Verfügung stehen. D. h. sie bzw. er fühlt sich oft machtlos infolge dieser Interessenskonflikte. Zwar hat sie bzw. er ausreichend Ideen, die Security-Kommunikation zu fördern – infolge des Drucks, den sie bzw. er verspürt, ist sie bzw. er jedoch äußerst dankbar für alle Werkzeuge, die ihr bzw. ihm als verlängerter Arm ihrer bzw. seiner Rolle von Außen angetragen und zur Verfügung gestellt werden. D. h. sie bzw. er braucht Tools wie die LS, um dem eigenen Anspruch von Awareness als „Sicherheits-Sozialarbeit" zu genügen, muss aber aufpassen, dass sie bzw. er den Kolleginnen und Kollegen nicht vermittelt, dass sie in Bezug auf Sicherheit nichts mehr unternehmen müssten, wenn diese die LS durchlaufen haben werden.

Mit diesem Bild entspricht sie bzw. er am ehesten dem Typus „Streetworker" oder „Inspektor Columbo" aus der Studie „Aus dem Abwehr in den Beichtstuhl" [17] (s. dort S. 34-39).

Mit Perspektive dieser Typologie wäre es sinnvoll, die LS auf eine typologische Passung hin zu untersuchen, verbunden mit der Fragestellung, inwieweit die Lebens- und Arbeitswelten bzw. Ansprüche dieser Prototypen in den LS abgedeckt sind, und dem Vorschlag, eine derartige Kompatibilität in der dritten, im Rahmen dieses Projektes vorgesehenen, Studie zu evaluieren.

Kapitel	6.1.1	6.1.2	6.1.3	6.1.4	6.1.5	6.1.6
LS **Bewertungskriterien**	Sicher zuhause wohnen & arbeiten	Kundendaten sicher managen in Cloud & Co.	Die 5 Phasen des CEO Fraud	Mobile Kommunikation, Apps & Co.	Cyber Pairs	Informationsklassifizierung
Themen-Passung KMU	++	0	++	+	+	-
Didaktischer Moderations-Zugang (Briefing)	++	+	+	++	++	+
Involvement (Spiel)	++	0	0	+	++	-
Diskurs-Qualität (LS)	++	+	+	+	++	+
Impact, Nachhaltigkeit	+	+	++	+	++	+
Bewertung Teilnehmende	++	+	+	+	+	-
Bewertung Awareness-Verantwortliche	++	0	+	+	++	--
Erforderlicher Mindestreifegrad (nach Kap. 7.3.6)	1	1	2-3	1	2-3	3
Bedarf Überarbeitung (Selbsteinschätzung)	--	+	0	-	-	+
GESAMT-BEWERTUNG	++	0	+	+	++	-

Bewertung: ++ sehr hoch + hoch 0 medium - niedrig -- sehr niedrig

Abb. 16: *Übersetzung der qualitativ-deskriptiven Evaluation aus Kapitel 6 in eine quantitative Matrix*

8 Fazit und Empfehlungen sowie Top-Learnings im Überblick

8.1 Fazit und Empfehlungen

Die hier teilnehmenden KMU und insbesondere die beiden, in denen Gruppendiskussionen stattgefunden haben und die für die in Kapitel 7.3 evaluierte Grundspannung „Enabling vs. Entmündigung“ stehen, sind in der hier vorgefundenen reinen Ausprägung dieser Spannung Ausnahmen. Es ist davon auszugehen, dass die überwiegende Anzahl an KMU Grundzüge beider Seiten aufweist und sich zwischen diesen extremen Polen einordnet.

Indes konnte mithilfe dieser Studie evaluiert werden, dass die LS des Projektes „ALARM Informationssicherheit“ mit den verbundenen Simulationen anspruchsvolle, weil vitalisierende, Awareness-Werkzeuge darstellen.

Das Thema Informationssicherheit – bzw. die Angst vor Risiken bzw. Versagen im Umgang mit ihnen – droht, die Menschen zu überwältigen. Awareness-Maßnahmen heben diese Verdrängung auf und insbesondere die Dimension des Enablings infolge der getesteten LS-Formate sorgen für eine notwendige Balance und Halt.

Vor allem die Stationen „Sicher zuhause wohnen & arbeiten“ und – mit einigen wenigen Abstrichen – „Cyber Pairs“ sowie „Mobile Kommunikation, Apps & Co.“ können im intendierten Sinne als Kommunikationsbeschleuniger überzeugen, die die Teilnehmenden in einen wertvollen Diskurs zum Thema Informationssicherheit involvieren.

Auch die anderen LS funktionieren ähnlich, jedoch nicht in jedem Umfeld gleich gut bzw. weisen diese noch Schwächen im Detail auf – vor allem in Bezug auf Verständnis von Terminologie, Themenclustern bzw. generelles Handling beim Spielen, einige wenige hinsichtlich der Gestaltung.

Wichtig ist: Kein LS funktioniert überall gleich gut. D. h. eine exakte Passung der LS zu definieren, wird durch die große kulturelle Heterogenität im KMU-Umfeld erschwert. Um die evaluierten Unterschiede so auszugleichen, dass eine gut darstellbare, quantitative Aussage (s. Tabelle linke Seite) über Kompatibilität der LS zu Unternehmens- bzw. Sicherheitskultur getroffen werden kann, muss die Perspektive auf den Security Awareness-Reifegrad (s. Kapitel 7.3) gelenkt werden.

Eine zielgruppenaffine Ausdifferenzierung der LS – etwa vergleichbar mit „SecAware4School“, ein Forschungsprojekt, das Schülerinnen und Schülern, Lehrerinnen und Lehrern sowie Eltern ebenfalls via LS hinsichtlich Informationssicherheit bzw. Datenschutz sensibilisiert und bei dem im Kontext der Spielgestaltung bei den LS drei so genannte „Schwierigkeitsgerade“ analog der Klassenzugehörigkeit berücksichtigt wurden – kann nicht empfohlen werden, da im Projekt „ALARM Informationssicherheit“ eine derartige Diversifizierung nicht vorgesehen ist und auch der erwartete Benefit in keinem adäquaten Verhältnis zu einer erhöhten Nutzungsfrequenz bzw. der Ausweiterung der Kernzielgruppen stehen würde.

Eine gegebenenfalls als notwendig betrachtete Diversifikation kann vielmehr relativ unaufwändig über einen potenziellen Niveauausgleich jeweils individuell während der Moderation hergestellt werden, da die LS-Briefings diesbezüglich modular angelegt sind und die Moderation jeweils individuell ausgestaltet werden kann.

Trotz der weitgehenden Homogenität bei den Risiko- bzw. Schmerzpunkten der KMU, über die via KMU-Grundlagenstudie Informationssicherheitsthemen gerankt und in die vorliegenden sieben LS-Konzepte geflossen sind [2], konnte evaluiert werden, dass für die Einführung bestimmter LS ein höherer Awareness-Reifegrad essentiell ist, damit der intendierte Wirkungsgrad erreichbar erscheint.

Daher ist davon auszugehen, dass gerade gamifizierte Settings in Organisationen mit einem sehr geringen Security Awareness-Reifegrad andere Effekte auslösen als die ursprünglich intendierte Präventionsleistung.

Insbesondere die LS „Informationsklassifizierung“ wirkt in der aktuellen Form derzeit noch zu generisch. Da jedoch in den meisten KMU eine Klassifizierung (noch) nicht als Standardprozess etabliert ist, macht es kaum Sinn, das Thema kleinen und mittleren Unternehmen anzubieten.

Die Teilnahme an LS erzeugt in der Regel bei den Mitarbeitenden Bedarfe hinsichtlich weiterer Awareness-Maßnahmen eben zu jenen Themenwelten, die in den LS angerissen werden. Wenn das dort Thematisierte jedoch nicht zur Anwendung kommt, ist es sinnlos, einen Diskurs hierzu aufzumachen. Auch ein beabsichtigter Nudge in Richtung einer potenziellen Nutzung von Informationsklassifizierung würde beim evaluierten Status Quo vermutlich eher zu Reaktanz als zu positiven Effekten führen.

Vielmehr Sinn würde es machen, das Thema Informationen breiter darzustellen und in dem LS auf den Aspekt der Klassifikation zu verzichten. Auch der Thematisierung von „Informationen“ vs. „Daten“ mit dem Unterschied von Informationsschutz bzw. Datenschutz könnte Chancen eingeräumt werden, tatsächlich zur Anwendung zu kommen.

Auf Basis der Beobachtungen, Gruppendiskussionen und Fokus-Interviews mit den Awareness-Verantwortlichen wird hierbei versucht, die qualitativ-deskriptive Evaluation dieses Reports in eine möglichst übersichtliche und vergleichbare quantitative Matrix zu transformieren (s. Abb. linke Seite).


Erste Hilfe
Failure is always an option
U-BAHN
ALARM
Mobile Kommunikation, Apps & Co.

8.2 Zusammenfassung der Top-Learnings

1. Security Awareness wird von den Befragten als wichtiger Baustein der Informationssicherheit betrachtet und wirkt generell äußerst vitalisierend. Im Spielen sind alle Teilnehmenden motiviert, gut gelaunt und zugleich ernsthaft und konzentriert. Auch in der Nachbetrachtung während der Gruppendiskussionen geben sich alle die Mühe, ein produktives Feedback beizutragen.

2. Der Ansatz, Awareness mithilfe von Gamification auf ein Niveau zu heben, das Einbindung schafft und die Sensibilisierungsleistung lerntheoretischer Ansätze deutlich übersteigt, funktioniert gut. Das LS-Format wird ganz unmittelbar mit „klassischen Powerpointschlachten" oder „langweiligen Web Based Trainings" verglichen und von allen sich äußernden Teilnehmenden als wesentlich involvierender erlebt. Es bildet ein wichtiges Scharnier zwischen Mitarbeitenden und den Sicherheitsprofis bzw. Führungskräften. Vorstellen kann man sich auch weitere LS z. B. zum Themenfeld „Social Engineering", etwa spezielle Ansätze, in denen die einzelnen Kanäle wie Face-to-face, Telefon, E-Mail etc. singulär betrachtet werden, oder Themen wie Phishing, Zugangskontrolle bzw. Clear Desk.

3. Die den LS zugrunde liegende didaktische Methode nach dem Prinzip „Talking Security", der diskursiven Auseinandersetzung zum Thema, funktioniert reibungslos: Den Austausch beim Spielen hat man mehrheitlich genossen, vor allem dann, wenn sich in Selbstorganisation Kleingruppen oder Paare bilden und synchron zu den jeweils anderen sehr persönlich miteinander diskutieren. Positiv wird vor allem auch bewertet, dass Gespräche über „Situationen aus dem wahren Leben" durch die Spiele angeregt werden. Eine Passung als Simulation realer Arbeits- und Alltagsszenarien ist mithin durchaus gegeben.

4. Die in der KMU-Grundlagenstudie [2] evaluierten Schmerzpunkte, aus denen die LS-Themen entwickelt wurden, sind weitgehend passend, allerdings mit einigen Brüchen, die eine Überarbeitung erfordern: Die Themenaspekte „Cloud", „Kundendatenschutz" sowie „Informationsklassifizierung", aber auch „Verschlüsselung" sind zu sehr aus der Perspektive von Security-Entscheidern, nicht aber aus Sicht der Mitarbeitenden gedacht.

5. Die aus den Security-Schmerzpunkten hergeleiteten Themen der LS unterscheiden sich nicht oder nur kaum von denen der Großunternehmen – aber: Diese Übereinstimmung betrifft die Cover-Ebene, d. h. lediglich oberflächlich betrachtet. Auf der Impact-Ebene – d. h. in Bezug auf das Verständnis einer oftmals unklaren Informationssicherheits-Terminologie und den darunter versammelten Detailinhalten eines LS – werden deutliche Unterschiede zu Konzernkulturen gewahr, und zwar insofern, dass die Perspektive insbesondere hinsichtlich der Abwehr der Risiken in vielen Fällen hier und dort eine andere ist. Wenn z. B. in KMU diskutiert wird, ob ein CEO Fraud allein durch die Ausgangslage einer übersichtlichen Belegschaft, in der gegebenenfalls jede/r jede/n kennt, zu verhindern wäre, geht ein solches Beispiel völlig an der Realität von global agierenden Großunternehmen vorbei.

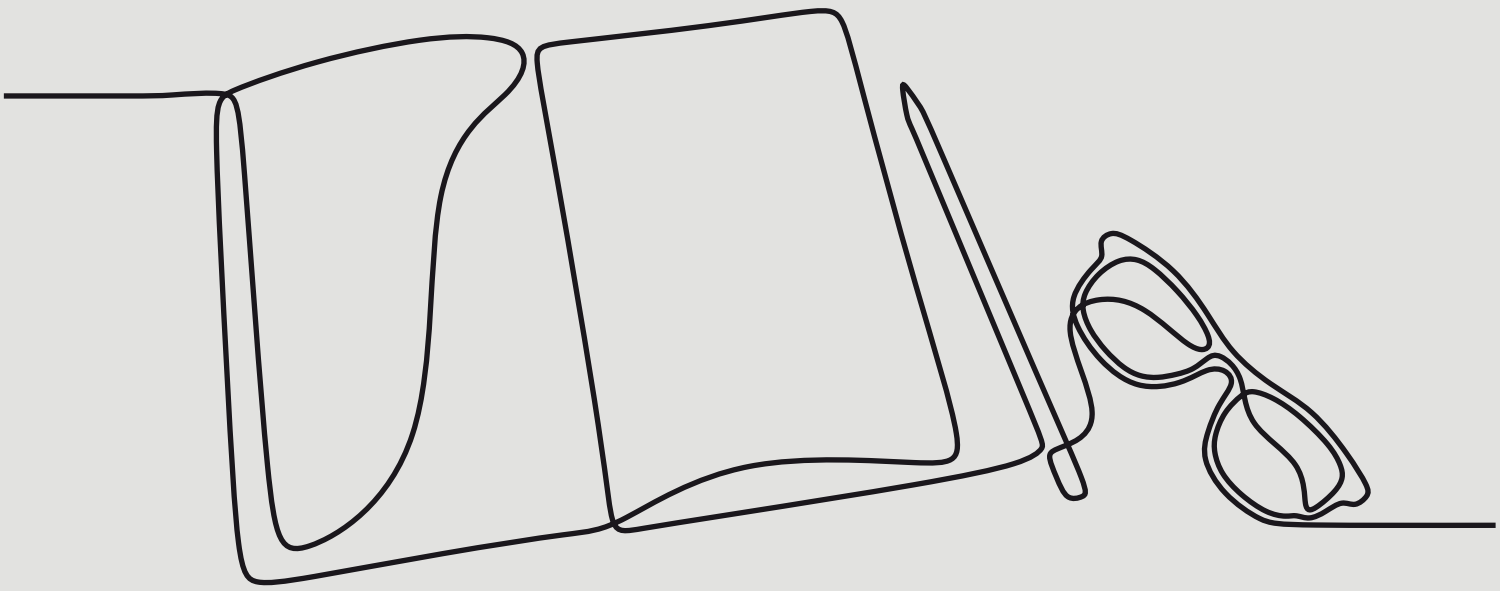
6. Kein KMU ist so wie das andere: Die Perspektive auf Diversifizierung in Bezug auf Unternehmens- und Sicherheitskultur von KMU darf sich nicht nur auf Größe, Umsatz, Branche, lokale oder regionale Besonderheiten beschränken. Die individuellen Ausprägungen, aus denen sich schließlich Sicherheitskultur herleitet, sind so divers, dass nicht jede Awareness-Maßnahme bei jedem Unternehmen funktioniert. Dies hat Auswirkungen auf die Passung der LS, für deren Kompatibilität idealerweise ein Reifegrad-Modell herangezogen werden sollte.

7. Der Awareness-Reifegrad in KMU korreliert mit der digitalen Autonomie der Mitarbeitenden. Awareness darf sich nicht auf rein digitale Kanäle beschränken, jedoch erhöht der Umgang mit digitalen Werkzeugen das Risiko-Potenzial in jeder Organisation. Ein reifer Umgang verlangt dann nicht nur ein Enabling in Bezug auf die digitalen Tools, sondern auch mit den Sicherheitsfallstricken, die diesen inhärent sind. Awareness ist mithin als Enabling verknüpft mit dem digitalen Fortschritt und der digitalen Autonomie von Organisationen bzw. Mitarbeitenden.

8. Security Awareness-Maßnahmen sind in Unternehmen, die die digitale Autonomie ihrer Mitarbeitenden nicht fördern, wirkungslos: Mitarbeitende, denen nicht zugetraut wird, sich verantwortungsbewusst zu verhalten, fühlen sich entmündigt. Sicherheit durch Unterbindung von Entscheidungsfreiheit kann zu Reaktanz und diese wiederum zu neuen Sicherheitsvorfällen führen, sprich: Mitarbeitende verweigern dann unbewusst Verantwortung oder boykottieren Sicherheitsmaßnahmen.

9. Security Awareness ist auch „Sozialarbeit": Sensibilisierung benötigt Vorbilder (Management) und den Diskurs – auch mit den Führungskräften. So genannte Quickwin-Tipps, die Awareness mit einem veraltetem Lerntheorie-Verständnis auf eine reine Informationsveranstaltung zu beschränken versuchen – so, wie sie z. B. das BSI immer noch lanciert [18]– ist äußerst kontraproduktiv. Gerade Delegation an z. B. Tool-Anbieter mit lerntheoretischer „Plattform-Awareness" wird angesichts der Heterogenität von Sicherheitskulturen in KMU nicht nachhaltig funktionieren. Ein sich entwickelnder Reifegrad hängt daher unter anderem auch von der passenden Auswahl der Sensibilisierungstools als Stellvertretende der Security-Organisation und -Handelnde sowie dem Zusammenwirken der Werkzeuge im Mix ab. Ein LS alleine macht noch nicht die „Awareness-Musik."

10. LS schaffen soziale Räume: Sie liefern nicht nur ein Awareness-Verspechen, sondern den Anwendenden die Dramaturgie für den Sensibilisierungsprozess sowie darüber hinaus auch hinsichtlich einer sozialen Balance bei hybridem Arbeiten gleich mit.



Literatur

[1] www.known-sense.de/security-arena. Zugriff: 11.10.2022

[2] Scholl, M. (Hrsg.), Qualitative Wirkungsanalyse Security Awareness in KMU – Tiefenpsychologische Grundlagenstudie im Projekt »ALARM Informationssicherheit«. Wildau: Technische Hochschule Wildau, 2021

[3] https://alarm.wildau.biz/. Zugriff: 11.10.2022

[4] http://s522854922.online.de/SecurityArenaThemenueberblick.pdf. Zugriff: 11.10.2022

[5] Kolarow, J., Entwicklung eines analogen Lernformates für die Schulung von Compliance-Inhalten unter Berücksichtigung lernpsychologischer Faktoren, Masterthesis, Köln: Rheinische Fachhochschule Köln, 2019, S. 44 ff.

[6] known_sense, DSV Gruppe, EnBW , <kes>, nextsolutions, Pallas (Hrsg.), Entsicherung am Arbeitsplatz. Die geheime Logik der IT-Security in Unternehmen, Köln: known_sense, 2006

[7] www.knowbe4.com/security-culture-maturity-model. Zugriff: 11.10.2022

[8] www.sans.org/security-awareness-training/resources/maturity-model/. Zugriff: 11.10.2022

[9] www.treesolution.com/news/capability-maturity-model-der-awareness. Zugriff: 11.10.2022

[10] www.treesolution.com/security-awareness-radar. Zugriff: 11.10.2022

[11] Watzlawick, P., Beavin, J. H., Jackson, D. D., Menschliche Kommunikation. Formen, Störungen, Paradoxien. Bern: Huber, 2000

[12] Zerr, K., Positive Einstellung mündet in sicherheitskonformes Verhalten. In: Helisch, M.. Pokoyski, D. (Hrsg.), Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Wiesbaden: Springer Vieweg, 2009

[13] known_sense, LanXess, TH Wildau, <kes> (Hrsg.), Bluff me if you can – gefährliche Freundschaften am Arbeitsplatz. Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr, Köln: known_sense, 2015

[14] Montaño, D. E., Kasprzyk, D. , Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In: Glanz, K., Rimer, B. K., Vishwanath, K.: Health behavior: Theory, research, and practice, S. 95 ff., Hoboken: Jossey-Bass, 2015

[15] Rasch, G., Probabilistic models for some intelligence and attainment tests. Copenhagen: Danish Institute for Educational Research, 1960

[16] Fertig, T., Schütz, A., Weber, K., Forschung zur Sensibilisierung der Beschäftigten von Unternehmen für Informationssicherheit, Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt, 2022, www.researchgate.net/publication/342838321_Towards_an_Information_Security_Awareness_Maturity_Model. Zugriff: 11.10.2022

[17] known_sense, EnBW, <kes>, Pallas, SAP, Sonicwall, Steria Mummert Consulting, Trendmircro (Hrsg.), Aus der Abwehr in den Beichtstuhl. Qualitative Wirkungsanalyse CISO & Co., Köln: known_sense, 2008

[18] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Cyber-Sicherheit für KMU. Die Top 14 Fragen, Bonn: BSI, Referat WG 23, 2022

Technische Hochschule Wildau
Technical University of Applied Sciences

known_sense

Security Awareness und Gamification mithilfe von Lernszenarien

Seit 2004 werden Formate mit spielbasierten Prinzipien (Serious Games) bei der Sensibilisierung von Mitarbeitenden in Bezug auf Informationssicherheit bzw. Datenschutz eingesetzt. Seit 2006 forscht die Awarenessagentur known_sense unter anderem zu diesem Thema und seit 2015 die Technische Hochschule (TH) Wildau, die über zahlreiche Projekte gemeinsam mit dem Studienpartner known_sense dazu beigetragen hat, dass heutzutage ein erlebnisorientiertes Awareness-Training mit spielebasierten Elementen bereichert werden kann, um die Menschen aktiv in lebendige Lernszenarien einzubinden zu können.

Seit 2020 entwickelt die TH Wildau im Rahmen des vom Bundesministerium für Wirtschaft und Klimaschutz geförderten Projektes „Awareness Labor KMU (ALARM) Informationssicherheit“ gemeinsam mit Unterauftragnehmern und assoziierten Partnern Security Awareness-Werkzeuge mit dem Ziel, die bundesweite Verbesserung der Security Awareness in KMU und damit eine generelle Erhöhung des IT-Sicherheitsniveaus in Deutschland voranzutreiben. Hierzu wird ein Gesamtszenario zur Sensibilisierung und Unterstützung der KKU/KMU für Informationssicherheit bis hin zu deren Selbsthilfe aufgebaut. Im Projekt werden 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 entwickelt.

Die Entwicklung von Lernszenarien im Projekt »Awareness Labor KMU (ALARM) Informationssicherheit« wird u. a. von quantitativer und qualitativer Forschung sowie Tests begleitet. Die Ergebnisse dieser Zwischenschritte werden miteinander verglichen und in Kontext zueinander gesetzt. Die hier vorliegende tiefenpsychologische Wirkungsanalyse ist die zweite einer Reihe von insgesamt drei qualitativen Studien. Nach einer Analyse des Ist-Zustands des derzeitigen Security Awareness-Niveaus in KMU im Sinne einer Grundlagenstudie zum Auftakt im Jahr 2021 werden hier die im Projekt entwickelten analogen Lernszenarien als Prototypen getestet, um bis zum Projektende im September 2023 allen KMU optimierte Versionen zur Verfügung stellen zu können.

ISBN 978-3-949639-03-6