ALARM
Awareness Labor KMU
Informationssicherheit

Qualitative Wirkungsanalyse Security Awareness in KMU

Tiefenpsychologische Grundlagenstudie im Projekt
»Awareness Labor KMU (ALARM) Informationssicherheit«

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Bibliographische Informationen der Deutschen Nationalbibliothek

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

Qualitative Wirkungsanalyse Security Awareness in KMU

Tiefenpsychologische Grundlagenstudie im Projekt »ALARM Informationssicherheit«

Impressum

Herausgeberin und Kontakt

Prof. Dr. Margit Scholl
Technische Hochschule Wildau
Hochschulring 1
15745 Wildau

alarm@th-wildau.de

Diese tiefenpsychologische Wirkungsanalyse ist die erste 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 Energie (BMWi) gefördert.

Projektlaufzeit

01.10.2020 – 30.09.2023

Die Studie basiert auf anonymisierten Tiefeninterviews, die von known_sense als Unterauftragnehmer der TH Wildau innerhalb des Projekts mit KMU von Januar bis März 2021 durchgeführt wurden. Die Studienergebnisse wurden von known_sense im April und Mai 2021 zusammengefasst und mit dem Forschungsteam Scholl der TH Wildau beraten.

Das BMWi hat die Veröffentlichung im August 2021 freigegeben.
Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie unter dem Förderkennzeichen 01MS19002A gefördert.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.
Verantwortlich für Inhalt und Gestaltung mit Ausnahme von Vorwort und Titelgrafik:

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

Feldarbeit | Analyse | Autoren:

Dietmar Pokoyski | Dipl.-Psychologin Ivona Matas |
Dipl.-Psychologin Ankha Haucke

Bilder

Abbildungen 1-15 siehe jeweilige Quellen
Titelgrafik: TH Wildau
Illustrationen: Simple Line via Shutterstock.com

August 2021

ISBN 978-3-949639-00-5

Das Projekt »Awareness Labor KMU (ALARM) Informationssicherheit« ist Teil der Initiative „IT-Sicherheit in der Wirtschaft“ im Förderschwerpunkt Mittelstand-Digital.

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand 4.0-Kompetenzzentren, der Initiative „IT-Sicherheit in der Wirtschaft“ und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de und www.it-sicherheit-in-der-wirtschaft.de.

Inhaltsverzeichnis

Ein Vorwort mit Einführung und Zusammenfassung der Studie: Mehrwert für KMU

Führungskräfte und Mitarbeitende sehen sich stolz als Team mit hoher Identifikation und engen Bindungen in ihrem kleinen und mittelgroßen Unternehmen (KMU). Mit hochwertigen Produkten, flexiblen Lösungen und beständigen Innovationen versucht man, gemeinsam am Markt zu bestehen. Gegenseitiges Vertrauen wird innerhalb der „familiären Kultur“ gelebt. Doch wie sieht es mit der *Informationssicherheit* (information security) und dem entsprechenden *Bewusstsein* (awareness) in deutschen KMU aus? Die hier von known_sense im Auftrag der TH Wildau vorgelegte tiefenpsychologische Grundlagenstudie will Licht ins Dunkel bringen und gleichzeitig mit ihren Empfehlungen einen Mehrwert für KMU aufzeigen.

Die Studie offenbart, dass der Begriff *Informationssicherheit* für viele noch diffus ist und nicht selten Experten und Dienstleistern zugeordnet wird. Zukünftig sollte daher die persönliche Wahrnehmung auf die *eigene Verantwortung* für Informationssicherheit am Arbeitsplatz geschärft werden. Zudem verdeutlichen die von den Interviewten genannten relevanten Themen, dass der Awareness-Reifegrad noch deutlich ausgebaut werden kann, denn auf den ersten beiden Plätzen liegen die altbekannten Problemfelder *Passwortsicherheit* und *Phishing-Attacken*. Damit wird deutlich, dass in KMU verstärkt *für alle* eine Bewusstseinsbildung (awareness raising) für Informationssicherheit stattfinden sollte. Gerade während der Pandemie sind jedoch Informationssicherheitsthemen in den Hintergrund geraten und werden häufig von Existenz- und Gesundheitsfragen dominiert. Doch zeigen immer wiederkehrende Beispiele, dass Cyber-Attacken ebenfalls existenzbedrohlich für KMU werden können.

Risiken von außen

Unabhängig davon wird in der vorliegenden Studie die Informationssicherheit auch in KMU zunehmend als wichtig angesehen. Sie wird jedoch in ihrer Wahrnehmung überwiegend durch Risiken von außen wie Cyber-Attacken, gesetzliche Regularien und Kundenanforderungen bestimmt. Das ist verständlich, wenn z. B. bedacht wird, dass Regulierungen eine erhebliche Herausforderung für das Informationssicherheitsmanagement in Unternehmen darstellen können und die neuen Anforderungen durch die EU-weite Datenschutz-Grundverordnung organisationsübergreifende Auswirkungen haben. Es müssen jedoch auch *innere Faktoren* zur Absicherung der Informationssicherheit erkannt werden. Hier ist in KMU der Spagat zu bewältigen, einerseits über Fehler und Versäumnisse reden zu können (sogenannte „Fehlerkultur“ der Unternehmen) und andererseits bei Verstößen nicht immer ohne Konsequenzen zu bleiben, was u. a. einen Imageverlust des Unternehmens bedeuten kann.

Durch die überschaubare Organisationsgröße, das gegenseitige gute Kennen und der persönliche Umgang wird in KMU *intuitiv* eine *diskursive Awareness* genutzt, somit über Vorfälle und Risiken zeitnah gesprochen. Das ist meines Erachtens ein wichtiger innerer Faktor, um eine anhaltende Sensibilisierung zu etablieren. Er reicht allein aber nicht für eine tatsächlich nachhaltige Bewusstseinsentwicklung für mehr Informationssicherheit aus. Für eine nachhaltige Sensibilisierung fehlt in KMU bislang oft die Etablierung einer *Strategie* für Informationssicherheitsbewusstsein in allen Tätigkeitsbereichen. Eine solche Strategie würde auch Fundament der notwendigen Sicherheitskultur in KMU sein.

Wissensvermittlung nicht ausreichend

Ganzheitliche Awareness-Konzepte, wie im vom BMWi geförderten Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ vorgesehen, oder ein Awareness-Rahmenprogramm mit dokumentierter Strategie kommen bisher in den befragten KMU ebenso wenig zum Einsatz wie Awareness-Messungen oder andere Evaluationen im Kontext der Sensibilisierung von Mitarbeitenden. Aktivitäten für mehr Awareness werden bislang oft nur in Form einer reinen Wissensvermittlung verstanden. Aus der Forschung wissen wir allerdings, dass dies zu kurz greift. Die Studie verdeutlicht daher das Drei-Ebenen-Prinzip *Wissen*, *Wollen*, *Können* für mehr Informationssicherheitsbewusstsein und beschreibt konkret Vorteile für Unternehmen sowie konkrete Ansatzpunkte für eine gezielte Personalentwicklung in KMU.

Erste Schritte in Richtung der Etablierung einer Sicherheitskultur werden von wenigen KMU durch den Kauf von kommerziellen, digitalen Awareness-Trainings gegangen. Diese KMU mussten allerdings feststellen, dass solche nicht an das Unternehmen angepassten Produkte wenig involvierend sind. Tatsächliche Wirkung können Awareness-Trainings meiner Meinung nach nur entfalten, wenn sie die Menschen emotional berühren und in ein interaktives Erleben mit diskursiver Teilhabe eingebettet sind.

Dazu stellt die Studie eine generalisierte Typologie mit fünf prototypischen Strategien im Umgang mit dem Thema *Informationssicherheit* bereit: IT-Kapitän/in, Vorfall-Experte bzw. -Expertin, verständnisvoller Tröster/verständnisvolle Trösterin, IT-Notfallsirene und Volldelegierer/in. Obwohl dies eine sehr grobe Klassifizierung ist, macht sie dennoch die Einschätzung von Schwachstellen und den Bedarf nach personalisierten Schulungen in den KMU sichtbar. Dies ist für die Unternehmen von großer Bedeutung, um eine passende, für die Mitarbeitenden und Führungskräfte kompatible Sensibilisierungsmaßnahme entwickeln und für eine Nachhaltigkeit der Maßnahme auch Mitarbeitende und Führungskräfte als Multiplikatoren für Schulungen oder Sicherheitsbotschafter/innen gewinnen zu können. KMU müssen dies als Prozess und nicht als Einzelaktion verstehen.

Spielebasierte Elemente

Heutzutage kann ein erlebnisorientiertes Awareness-Training mit spielebasierten Elementen bereichert werden, um die Menschen aktiv in ein Lernszenario einzubinden („Serious Games“). Die Studie offenbart, dass es in deutschen KMU noch Vorbehalte gibt: das Spielerische darf nicht im Vordergrund stehen, wenn Akzeptanz erreicht werden soll. Nach den vielfältigen praktischen Erfahrungen meiner Forschungsgruppe mit unterschiedlichen Zielgruppen sind solche Vorbehalte in Deutschland nicht selten vorzufinden und erst, wenn die Menschen die erlebnisorientierten interaktiven Lernszenarien tatsächlich durchführen, erkennen sie den Mehrwert zur Erreichung von mehr Sensibilisierung und nachhaltiger Achtsamkeit für Informationssicherheit.

Die Ergebnisse dieser Studie bilden im Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ die Ausgangsbasis für die Entwicklung von neuen, an die KMU angepassten Sensibilisierungsmaßnahmen. Ihr Ziel und damit der Mehrwert für KMU ist die Bereitstellung integrativ verzahnter Maßnahmen für eine systematische Sensibilisierung, die eine Sicherheitskultur tatsächlich zu entwickeln hilft und sich von gescheiterten klassischen Schulungen unterscheidet.

Prof. Dr. rer. nat. Margit C. Scholl

Juli 2021

1. Einleitung mit Ausgangslage

1.1 Ausgangslage KMU

Laut Definition der EU-Kommission fallen Unternehmen unter die Bezeichnung KMU (kleine und mittlere Unternehmen), wenn sie maximal 249 Mitarbeitende beschäftigen, einen jährlichen Umsatz von höchstens 50 Millionen Euro erwirtschaften bzw. über eine Bilanzsumme von höchstens 43 Millionen Euro verfügen [1]. KMU gelten als Wirtschaftstreiber, weil die Einrichtung neuer Arbeitsplätze vorwiegend auf Unternehmen dieser Größenordnung zurückgeht [2].

KMU erheben, verarbeiten, übertragen und nutzen zahlreiche sensible Daten mithilfe digitaler Lösungen. Dabei wird ihnen jedoch allzu häufig eine gewisse Sorglosigkeit in Bezug auf Datenschutz, Informationssicherheit, Unkenntnis bzw. Verletzung von betrieblichen Richtlinien sowie nichtexistente bzw. lückenhafte Sicherheitsrichtlinien zugeschrieben, die eine Risikoerhöhung zur Folge hat. Die vielfältigen Schwachstellen sind Sicherheitsmängeln gleichzusetzen, die zukünftige verzögerte Folgen für KMU sowie KKU (Kleinst- und Kleinunternehmen) haben können. „Wenn wir einmal in ein Netzwerk eingedrungen waren, konnten wir dort machen, was wir wollten – wir waren praktisch wie Gott in den IT-Systemen“, sagt der White-Hat-Hacker Michael Wiesner in dem Report Cyberrisiken in produzierenden Gewerbe [3]. Denn auch in KMU gilt genauso wie in Großunternehmen: Der Mensch ist und bleibt die größte Schwachstelle der Informationssicherheit und ist gleichzeitig deren größte Chance [3] hinsichtlich einer Resilienz im Sinne bewusst angewandter Abwehrmaßnahmen wie z. B. Security Awareness (Sicherheitsbewusstsein).

1.2 Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“

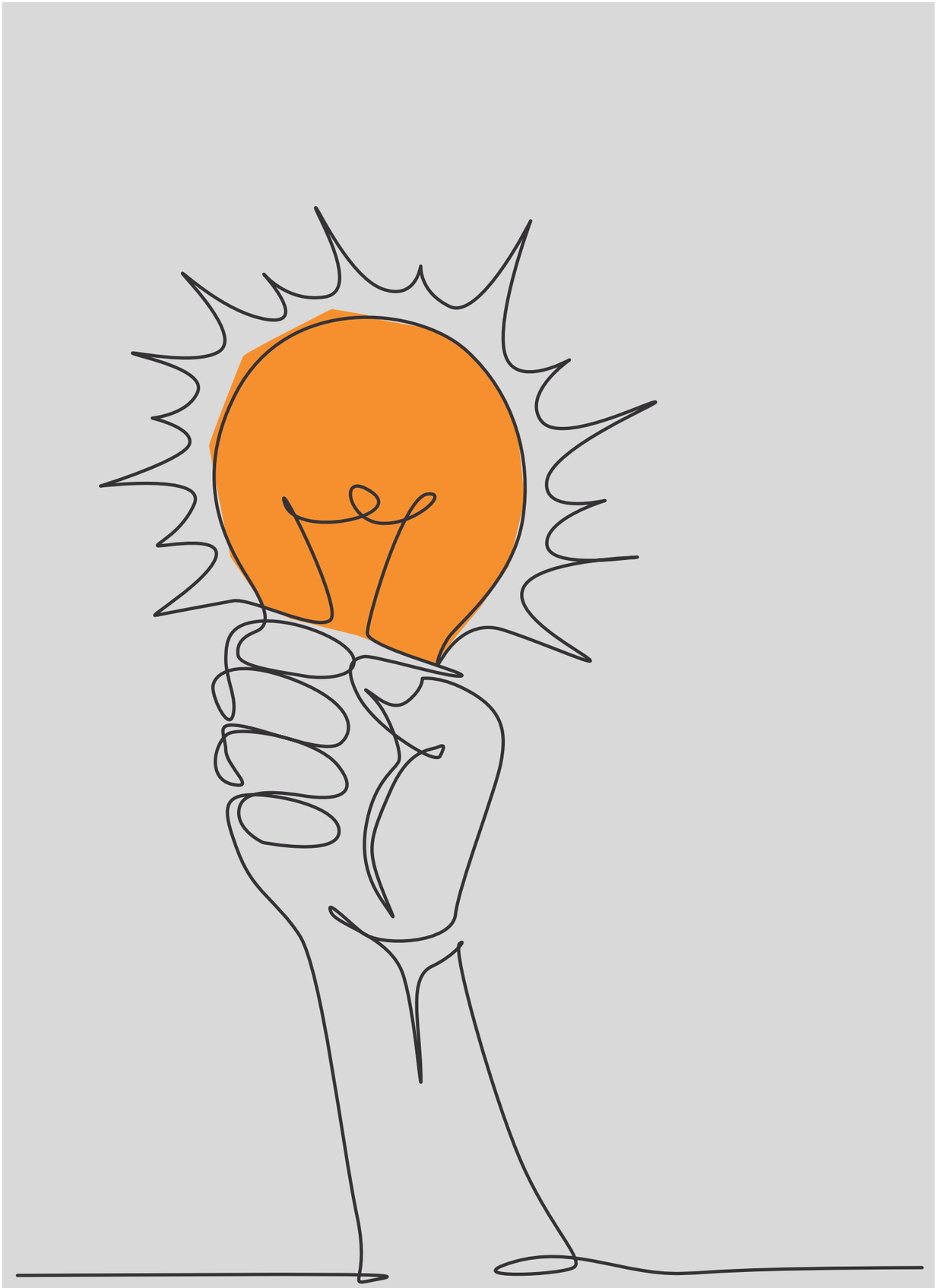
Vor diesem Hintergrund entwickelt die Technische Hochschule (TH) Wildau im Rahmen des vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Projektes „Awareness Labor KMU (ALARM) Informationssicherheit“ gemeinsam mit Unterauftragnehmern und assoziierten Partnern bis September 2023 Security 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 Prozessszenario für Informationssicherheit mit analogen und digitalen erlebnisorientierten Szenarien, sowie „Vor-Ort-Angriffen“ und weiteren Überprüfungen entwickelt.

Das Gesamtszenario soll der dringend notwendigen Sensibilisierung von Führungskräften und Mitarbeitenden und gezielten Personalentwicklung in KMU/KKU dienen, wie sie derzeit breitenwirksam noch nicht vorhanden ist. Dazu wird IT-Sicherheit im Zusammenhang mit den zunehmend digitalen Arbeitsprozessen konkret (be-)greifbar gestaltet, gleichzeitig werden die Menschen emotional berührt und aktiv in die Entwicklung von Maßnahmen einbezogen. So soll eine nachhaltige und unternehmensweite Informationssicherheitskultur aufgebaut werden [4].

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 der Auftakt einer Reihe von insgesamt drei qualitativen Studien, die innerhalb der Projektlaufzeit um qualitative Konzept- und Produkttests der sukzessive zu entwickelnden Lernszenarien für KMU ergänzt werden.

Ziel der Auftaktstudie ist die Analyse des Ist-Zustands des derzeitigen Security Awareness-Niveaus in KMU im Sinne einer Grundlagenstudie. Damit sollen systematisch defizitäre Bereiche relevanter Geschäftsprozesse, Wissensstand, Kompetenzprofile, Bedarf der beteiligten Organisationen, Zielgruppen und Passung bestehender Werkzeuge, die bisher vornehmlich in Großunternehmen eingesetzt werden, erfasst werden. Hierfür werden u. a. Kommunikationskanäle, Sicherheitskultur, zentrale Themen der Informationssicherheit und die Ansprachemöglichkeiten der Zielgruppen identifiziert und somit der spezifische Sensibilisierungsbedarf definiert, der in KMU zur Verbesserung der Informationssicherheit beitragen soll. Außerdem werden dort, wo Gegenüberstellungen sinnvoll erscheinen, auf Basis eines Vergleichs zu internen Wirkungsanalysen von known_sense-Kunden die Unterschiede zu Security Awareness in Großunternehmen herausgestellt.

Eine abschließende Bewertung zum allgemeinen Zustand der Informationssicherheit war explizit nicht Intention der vorliegenden Studie. Auch auf die Abfrage hinsichtlich eines Information Security Management System (ISMS) als Grundlage wurde zugunsten von Fragen bzgl. des persönlichen Erlebens der Informationssicherheit und deren konkrete Maßnahmen verzichtet.



1.3 Die Technische Hochschule Wildau (TH Wildau) als Projektauftragnehmer

Die TH Wildau des Landes Brandenburg ist seit ihrer Gründung im Jahre 1991 eine forschungsstarke Fachhochschule mit positivem Einfluss auf die Lehrqualität. Die Einheit von angewandter Forschung und Lehre ist für die TH Wildau ein zentrales Anliegen. Sie hat sich in vielen Drittmittelprojekten auch überregional als kompetenter und verlässlicher Partner erwiesen. Für die Forschungsgruppe Scholl der TH Wildau steht dabei immer die Anwendungsorientierung im Vordergrund, Forschung und Entwicklung (F&E) sowie Wissen- und Technologietransfer und Lehre gehören zusammen.

1.4 Die Firma known_sense als Unterauftragnehmer

Die Firma known_sense kümmert sich als Full-Service-Agentur mit Sitz in Köln um die Sicherheitskommunikation und insbesondere um Security Awareness bzw. Sicherheitskultur ihrer Kunden. Für Security Awareness-Kampagnen entwickelt known_sense individuelle, zur jeweiligen Kultur passende Sensibilisierungs-Tools und -Formate und bietet in diesem Rahmen auch Good Practice aus mehr als 100 Kampagnen mit 19 Jahren Erfahrung in 50 Ländern an. Die methodischen Ansätze sind tiefenpsychologisch (z. B. im Rahmen qualitativer Security-Wirkungsanalysen), systemisch, diskursiv, konstruktivistisch. Das Vorzeige-Tool bei known_sense ist das 2011 entwickelte Lernstationsformat „Security Arena“, das das Lernen aus der Einsamkeit von Online-Settings in diskursiv-lebendige Team-Formate überführt und ein Vorbild für die im Projekt „ALARM Informationssicherheit“ zu entwickelnden analogen Lernszenarien darstellt.

1.5 Exkurs: Security Awareness

Zum Verständnis der Studie erscheint es sinnvoll, Begriffe im Kontext von Security Awareness zu definieren und das Thema in Zusammenhang mit Informationssicherheit, spezifischer Methodik bzw. Disziplinen (z. B. Didaktik, Marketing, Veränderungsmanagement) und systemischer Kommunikation zu stellen. Grundlage hierfür ist ein von known_sense entwickeltes, umfangreiches Security Awareness-Rahmenwerk [5], das seit 2016 bei zahlreichen Kunden von known_sense immer dann zum Einsatz kommt, wenn Sensibilisierung über die Begrenztheit eines Security Awareness-Kampagnenkonzepts hinaus, mithin als permanente Lösung gedacht wird. Das Security Awareness Framework kann auch von Dritten lizenziert und mit den notwendigen Adaptionen in das eigene Information Security Management System integriert werden [6].

1.5.1 Treiber von Security Awareness

Information Security Awareness (Sensibilisierung der Mitarbeitenden zum Thema „Informationssicherheit“) gehört unter anderem zu den gesetzten Bestandteilen der Geschäftsabläufe auf allen Ebenen seriös agierender Organisationen. Gerade Bezugsgruppen wie Gesetzgeber, Gerichte, Kunden, weitere Business-Partner u. v. m. fordern nicht nur generelle Nachweise in Bezug auf Informationssicherheit, sondern zunehmend auch die einer erfolgreichen Sensibilisierung der Mitarbeitenden. Im juristischen Kontext ist dies u. a. für den Fall etwaiger Compliance-Verstöße notwendig [5].

So definiert der internationale Standard ISO 27001 [7] die spezifischen Anforderungen für ein ISMS. Durch das Einhalten des internationalen Standards soll

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

Die ISO 27001 fordert explizit auch die Schulung der Mitarbeitenden im Bereich der Informationssicherheit und der Security Awareness und definiert die Details einer derartigen Schulung unter dem Standard A.7.2.2 („Information Security Awareness, Education and Training“). Ferner sind in den Kapiteln 7.1 bis 7.4 verschiedene Aspekte von Schulung und Training bzw. Security Awareness beschrieben [7].

Zusätzlich sind Legislative, Kunden und Öffentlichkeit konkrete Treiber für Security Awareness [7].

1.5.2 Vorteile von Informationssicherheits-Sensibilisierung (Security Awareness Benefits)

Die kontinuierliche Implementierung von Security Awareness-Maßnahmen reduziert in überprüfbarer Weise nicht nur das geschäftliche Risiko von Unternehmen; sie erhöht darüber hinaus deren Attraktivität. Denn sowohl die Zusicherung von Sensibilisierungsmaßnahmen gegenüber Kunden als auch deren externe Kommunikation sichern den Unternehmen Wettbewerbsvorteile, weil sie positive Imagefaktoren generieren und das Vertrauen in das Unternehmen erhöhen [5].

Damit ist Security Awareness als Teil von Sicherheitskommunikation eine Voraussetzung für erfolgreiches Security Management. Die verschiedenen Maßnahmen der letzten Jahre haben die Unternehmenskulturen zahlreicher Organisationen im Hinblick auf Informationssicherheit sowie das sicherheitsrelevante Verhalten der Beschäftigten positiv beeinflusst [8]. Wenn man die Gründung des Dax-30 Roundtable Security Aware-

ness 2006 und die Aktivitäten der dortigen Mitglieder als Maßstab betrachtet, wird in den meisten Großunternehmen – aber auch vereinzelt bei KMU – Security Awareness seit etwa 15 Jahren über diverse Einzelmaßnahmen und planvoll gebündelt über Kampagnen (und zunehmend auch strategisch unterfüttert mit einer Entwicklung, die auf Persistenz abzielt) betrieben [9].

Mit der Umsetzung wirksamer und nachhaltiger Security Awareness-Maßnahmen ergeben sich verschiedene Vorteile für Unternehmen [5]:

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

1.5.3 Definition und Aufgaben von Security Awareness

In Bezug auf das Verständnis von Security Awareness existieren zahlreiche unterschiedliche Definitionen mit zum Teil sehr unterschiedlichen Nuancierungen. Der im Projekt „ALARM Informationssicherheit“ verwendete Begriff unterliegt der folgenden Definition [5]:

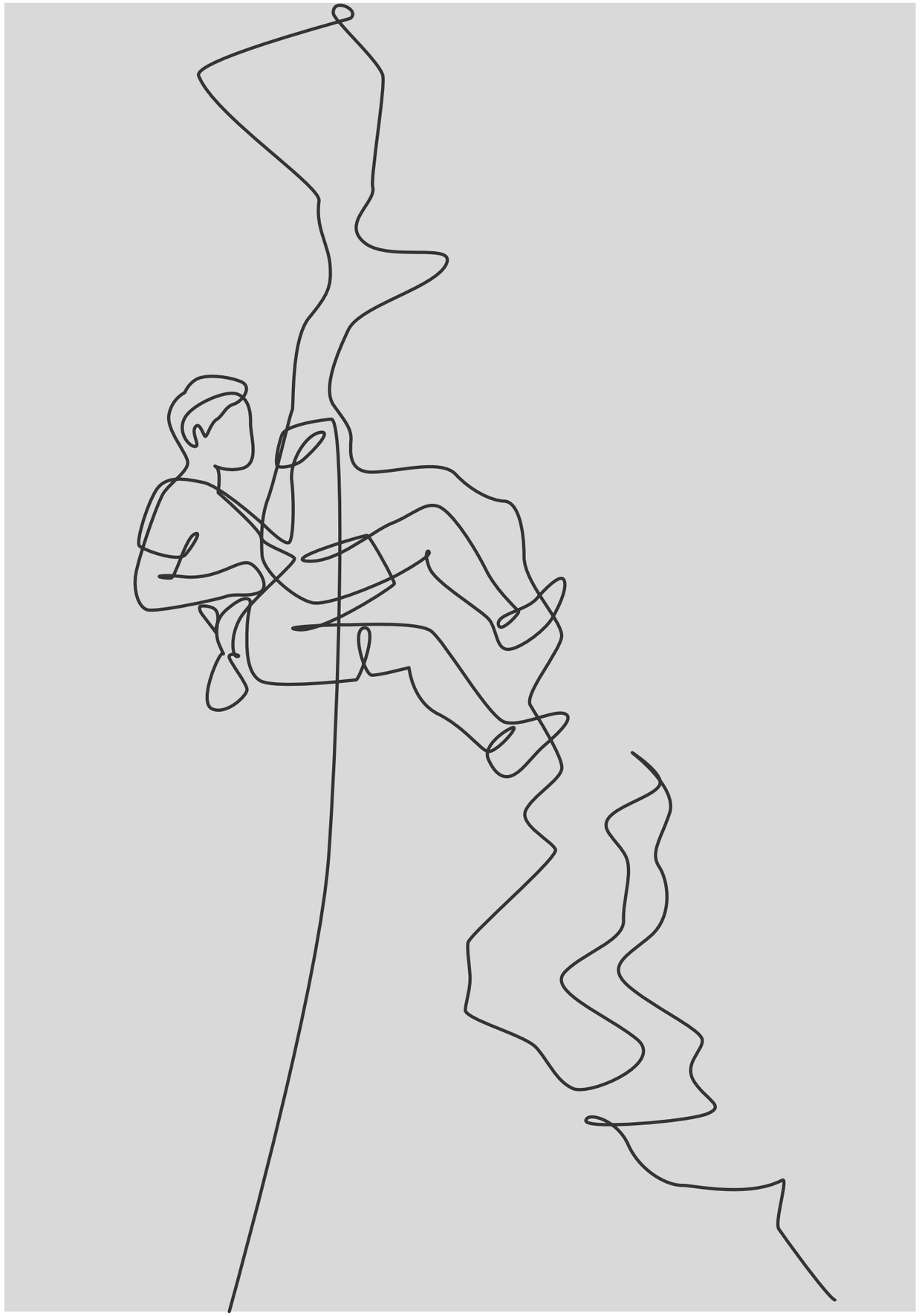
Security Awareness ist der Prozess einer methodischen, dauerhaften und nachhaltigen Bewusstseinsbildung bei allen Beschäftigten zum Thema „Informationssicherheit“ mit dem Ziel, diese in einer dem Unternehmen und den Beschäftigten dienlichen Form zu überführen.

Aufgaben von Security Awareness sind u. a. [5]:

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

1.5.4 Definition Sicherheitskultur

Basierend auf diesen zuvor benannten Aufgaben ist Security Awareness sowohl Teil von Security Marketing und Security Kommunikation, die wiederum dem Begriff der Sicherheitskultur untergeordnet werden [5]. Daraus lässt sich ableiten, dass unter Sicherheitskultur die Gesamtheit der Überzeugungen und Werte von Individuen und Organisationen verstanden wird, bei denen eine Übereinkunft herrscht, welche Ereignisse Risiken darstellen bzw. mit welchen Mitteln diesen Risiken begegnet werden [5].



Sicherheitskultur unterliegt einem komplexen Lern- und Erfahrungsprozess, in dem sich gemeinsame Ziele, Interessen, Normen, Werte und Verhaltensmuster herausbilden, und ist daher als ein Teil der Unternehmenskultur zu verstehen, an der sichtbar wird, wie Beschäftigte mit Herausforderungen im Kontext Sicherheit umzugehen pflegen. Damit beschreibt sie auch die Art und Weise, wie Sicherheit am Arbeitsplatz organisiert wird, und gibt somit Einstellungen, Überzeugungen, Wahrnehmungen und Werte der Mitarbeitenden in Bezug auf Sicherheit wieder [5].

Der Begriff „Sicherheitskultur“ beschreibt ein dynamisches Phänomen, dessen Ausprägungen sich mit jedem maßgeblichen Ereignis in der Organisation verändern [5]. Dieser Entwicklung muss bei der Implementierung von Security Awareness-Maßnahmen Rechnung getragen werden.

Security Awareness ist nach der o. g. Definition mithin Teil der Sicherheitskultur und prägt darüber hinaus diese maßgeblich durch u. a. folgende Faktoren [5]:

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

1.5.5 Methoden für Security Awareness

Dabei existieren verschiedene Methoden zur Schaffung und Modellierung von Awareness, deren Inhalte, Ausführung und Erfolg u. a. vom Geschäftsmodell sowie der Unternehmens- und Sicherheitskultur abhängen.

Wichtig scheint uns auch der Hinweis auf Security Awareness als ein multidisziplinärer Bereich, an dem u. a. kognitive, emotionale und systemische Faktoren beteiligt sind [10].

Das heißt, die Schlüsselfaktoren von Security Awareness weisen Überschneidungen auf zum betrieblichem Bildungsmanagement bzw. zur Personalentwicklung, zur generellen Security-Kommunikation sowie zum Veränderungsmanagement und prägen die drei methodischen Ebenen von Security Awareness (known_sense spricht in diesem Kontext von „Layern“) [10]:

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

Ebene 1: Wissen (Lerntheorie)

Die klassische Kognition (Informationsverarbeitung) bildet die (Old School-)Grundlage von Security Awareness. Hierüber findet die informelle Wissensvermittlung in Bezug auf Security-Regeln, Richtlinien (Policies), Sicherheitsrisiken und möglicher Folgen von Sicherheitsverstößen statt. Dies geschieht in der Regel auf einer sichtbaren, d. h. nachweisbaren, faktischen Ebene (Cover-Story) [11] und gründet auf Methoden der klassischen Lerntheorie und Einsatz der klassischen Lehrmedien bzw. -formate [12].

Ebene 2: Wollen (Marketing)

Da Sicherheits- und Fehlerkultur ihren Ursprung in der Regel auf einer unbewussten, häufig nicht sichtbaren Ebene (Impact-Story) [11] haben und die reine Informationsvermittlung nicht ausreicht, um in Awareness-Prozessen eine nachhaltige, gerade auch motivierende Wirkung auszuüben, müssen bei sämtlichen Zielgruppen auch emotionale Faktoren adressiert werden (Ebene 2). Diese notwendige Bewegung der Ebene 2 von Security Awareness (Wollen) wird vor allem über den Einsatz von klassischen und innovativen Marketing-Instrumenten erreicht [12].

Ebene 3: Können (systemische Kommunikation)

Sicherheitskultur ist stets geprägt von der Interaktion mit Mitarbeitenden sowie Kunden und Partnern. Sicherheit umfasst demnach auch systemische Faktoren, dem Zusammenspiel in einer Organisation (und ihrer Außenkontakte) vor dem Hintergrund ihrer Unternehmenskultur. Die Besonderheiten dieses Zusammenspiels in der Ebene 3 (Können) lassen sich produktiv über systemische Kommunikation fördern. D. h., es geht hier auch im Sinne von „Empowerment“ (Verstärkung von Autonomie bzw. Selbstbestimmung) um das Einordnen und Einüben sicherheitskonformen Handelns. Dafür eignen sich insbesondere, dialogische Konstellationen (z. B. Teamformate) mit dem Ziel, soziale Handlungskompetenzen und einen für Awareness notwendigen Sicherheitsdiskurs unter den Beteiligten zu fördern, damit in der Awareness-Informationslogistik auch formlose, informelle Informationsflüsse (Flurfunk, z. B. Pausengespräche) eingebunden sind, die nicht von den Sicherheitsbereichen organisiert und kontrolliert werden.

Erst die durch das Marketing bedingte emotionale Ansprache (Ebene 2) und das systemische Einüben von Security relevantem Verhalten (Ebene 3) ermöglicht das Abrufen der Wissensbasis aus Ebene 1. Umgekehrt lassen sich die Lernphasen einer Know-how-Vermittlung (Ebene 1) erfolgreicher gestalten, wenn der Wissensvermittlung auch emotionale und systemische Aspekte inhärent sind. Denn spielerisches Lernen führt zu einer höheren Awareness-„Haltbarkeit“ als rein kognitives Lernen, das häufig als Arbeit wahrgenommen wird [12].

Formate und Instrumente der Ebene 1 sind z. B.

- klassisches E-Learning (z. B. Web Based Trainings – WBTs)
- klassische Präsenztrainings
- klassischer Textcontent (z. B. Artikel in Corporate Media wie etwa Intranet)
- Quickinfos (z. B. via E-Mail)

Formate und Instrumente der Ebene 2 sind z. B.

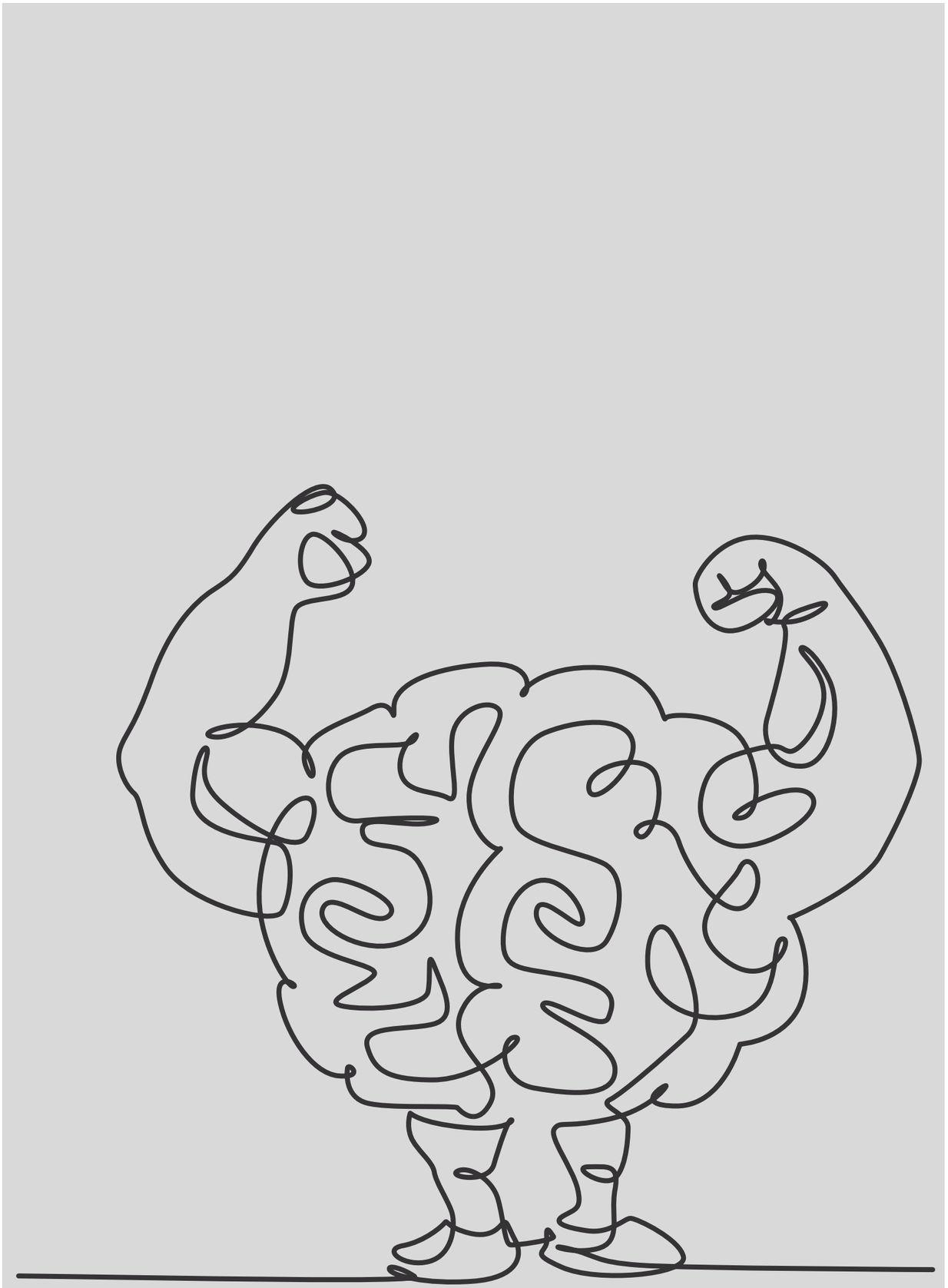
- Flyer und Quick Guides
- Poster, Aufsteller u. a. Visuals
- Videos, Podcasts etc.
- Mitarbeiter-Events
- Giveaways und Incentives
- weitere Marketing-Tools

Formate und Instrumente der Ebene 3 sind z. B.

- Moderationsinstrumente für diskursive Team-Settings, z. B. Moderationskartensets, Lernkarten
- Deep Dive Workshops u. a. zielgruppenspezifische Intensivtrainings mit Simulationen und weiteren diskursiven, gamifizierten bzw. interaktiven Elementen
- Simulationen, Lernstationen, Edutainment-Spiele
- (interaktive) Aktionen, Tests, Assessments

Eine derartige Typologie von Formaten existiert nicht in Reinform. D. h., die im Projekt „ALARM Informationssicherheit“ zu entwickelnden Lernszenarien sind grundsätzlich der Ebene 3 zuzuordnen und umfassen gleichzeitig didaktische und emotionale Awareness-Leistungen aus den Teildisziplinen Lerntheorie (Ebene 1) bzw. Marketing (Ebene 2).

Aus zahlreichen internen, tiefenpsychologischen Studien bei known_sense-Kunden (z. B. Tiefenpsychologische Konzeptanalyse mySecurity & Privacy Box bei T-Systems International) [13] sowie quantitativen Erhebungen im Kontext qualitativer und quantitativer Erfolgsmessung, die known_sense für weitere Kunden intern produziert hat, ergaben sich wichtige Faktoren für die Umsetzung der Methoden. Sämtliche Ebenen sollten wechselseitig im Sinne einer widerspruchsfreien Kommunikation an einer Kampagne beteiligt sein. D. h. auch, dass jedes Instrument mit jedem anderen verbunden sein sollte; die einzelnen Formate sollten auf die jeweils anderen einzahlen (d. h. für diese werben). Darüber hinaus muss eh ein diverses Portfolio an Formaten bereitgestellt werden, die unterschiedliche Lerntypen bzw. Zielgruppen und psychologische Verfassungen ansprechen.



2. Stichprobe, Untersuchungsdesign und Auffälligkeiten

2.1 Stichprobe der Untersuchung

Es wurden insgesamt 16 Probanden und Probandinnen aus KMU in 90-minütigen Online-Interviews befragt.

- Zur Durchführung wurden sichere WebEx-Räume durch die Forschungsgruppe Scholl der TH Wildau zur Verfügung gestellt.
- Ursprünglich waren zunächst 15 zweistündige Face-to-face-Interviews geplant, die aufgrund der Pandemie ausnahmslos online durchgeführt wurden. Auf Bitten der Geschäftsführungen der beteiligten KMU wurden die Online-Interviews um 25% (30 Minuten) gekürzt.
- Die Gespräche fanden größtenteils aus den Homeoffices heraus statt.
- Bei vier Interviews befanden sich die Gesprächspartner/innen am Arbeitsplatz im Unternehmen.
- Befragt wurden 6 Frauen und 10 Männer.
- Die teilnehmenden Pilotunternehmen gehören verschiedenen Branchen an (u. a. Software, Personalvermittlung, Anlagenbau).
- Die Interviews wurden im Zeitraum vom 10.02.2021 bis 12.03.2021 durchgeführt.

Funktionen der einzelnen Gesprächspartner/innen:

- Geschäftsführungen (GF):
  4 teilnehmende Assistent/innen der Geschäftsführungen bzw. Führungskräfte
  9 Teilnehmende, davon
  3 IT-Spezialisten/IT-Spezialistinnen
- Weitere Angestellte ohne Führungsfunktion bzw. Personalverantwortung: 2 Teilnehmende
- Auszubildende: 1 Proband/in

Alter der Probanden/Probandinnen:

- 18–25 Jahre: 1 Proband/in
- 26–35 Jahre: 6 Probanden/Probandinnen
- 36–45 Jahre: 4 Probanden/Probandinnen
- 46–55 Jahre: 3 Probanden/Probandinnen
- > 56 Jahre: 2 Probanden/Probandinnen

Arbeitsorte der Probanden/Probandinnen:

- Raum Berlin/Brandenburg
- Baden-Württemberg

Zitate der Probanden/Probandinnen:

Sind jeweils kursiv in orangen Balken gesetzt.

Methodik:

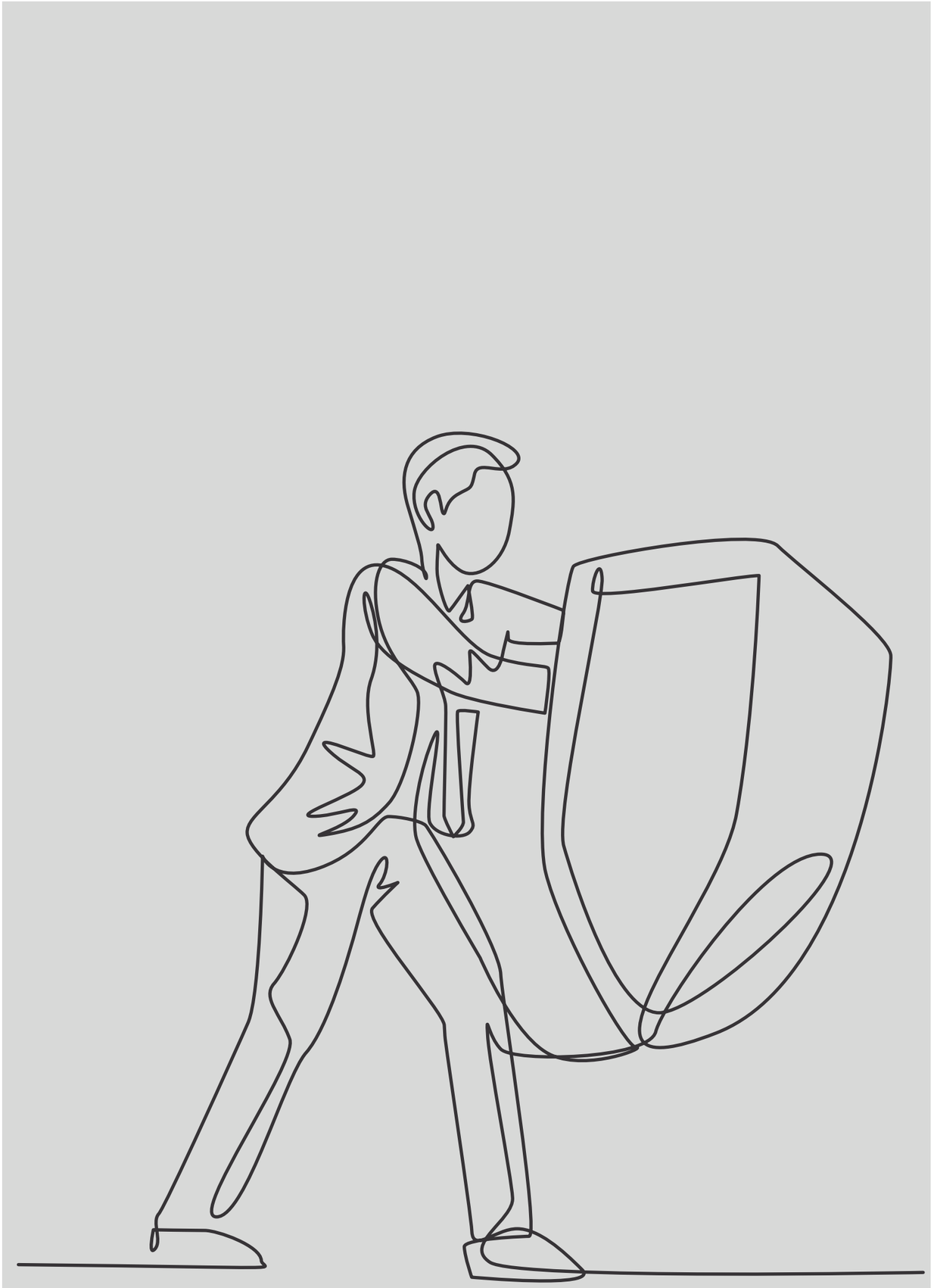
Morphologische Markt- und Medienforschung, ergänzt um Sekundärforschung, u. a. vergleichende Beschreibung bzw. Kennzahlen (Key Performance Indicators) unter Berücksichtigung interner Security Awareness-Kampagnen-Evaluationen durch known_sense bei sechs deutschen Großunternehmen unterschiedlicher Branchen von 2009 bis 2020.

Team des Unterauftragnehmers known_sense:

- Dipl. Psychologin Ankha Haucke
- Dipl. Psychologin Ivona Matas
- Dietmar Pokoyski (Geschäftsführer)

Wichtige Begriffe (weitere siehe Glossar)**:**

- **Tiefenpsychologie** fasst sämtliche psychologische Ansätze zusammen, die den unbewussten seelischen Vorgängen einen hohen Stellenwert für die Erklärung menschlichen Verhaltens und Erlebens beimessen. Die zentrale Idee ist hierbei, dass „unter der Oberfläche“ des Bewusstseins (etwa jenseits einer sog. Cover Story) in den „tieferen“ Ebenen (Layern) der Psyche weitere, unbewusste Prozesse ablaufen, die das bewusste Seelenleben (entspricht etwa der Impact Story) stark beeinflussen [11].
- **Morphologische Markt- und Medienpsychologie** hat seit den 1980er-Jahren und damit weit vor dem Marketing-Mainstream umfassende Modelle kreiert und weiterentwickelt, die bereits vor 40 Jahren aktuell aufkeimende Diskussionen und Anforderungen von Marketing und Kommunikation in systematischer und ganzheitlicher Weise aufgriffen. Das Grundprinzip ist es, die Produkt- bzw. Medienverwendungsformen, Markenbilder oder generell Settings (z. B. Alltagssituationen) mithilfe von Tiefeninterviews und einer bestimmten Beschreibungs-, Analyse- und Transformationsmethode als lebendige Formenbildung zu erfassen und darzustellen. Durch diese Perspektive wird sichtbar gemacht, inwiefern spezifische psychologische Motive (Verhalten, Visionen, Wünsche, Bedürfnisse etc.) komplexe Vermittlungen von psychischen Grundtendenzen



und -positionen sind, die z. B. known_sense speziell für den Bereich der Sicherheit aufgegriffen und weiterentwickelt hat [14].

- **Verfassungen** sind Modelle des **Verfassungsmarketings**, wie es die morphologische Markt- und Medienpsychologie betreibt. Psychologische Verfassungen werden dabei je nach Kontext des menschlichen Verhaltens betrachtet. D. h., Menschen verhalten sich nicht in allen Situationen gleich, wie es z. B. das klassische Zielgruppen-Marketing suggeriert. Zu unterscheiden ist beispielsweise, ob im Büro oder Homeoffice gearbeitet wird, elektronisch oder Face-to-face kommuniziert wird und zu welchen Tageszeit bzw. innerhalb welcher Settings Arbeitsprozesse stattfinden, z. B. ob dies am Vormittag, kurz vor oder nach der Mittagspause passiert und uns die Arbeit so aufhält, dass sie nach dem eigentlichen Feierabend erledigt werden muss. Diese und andere Kontexte geben unsere psychologischen Verfassungen als eine Art Stimmung vor, die unser Verhalten maßgeblich beeinflussen [15]. Das Verfassungsmarketing setzt also an Stimmungen, Bestimmungen, Zuständen, Bedingungen, Lebensgefühlen an, in denen sich Menschen befinden, die z. B. als Konsument/in Produkte kaufen oder eben mit Informationssicherheit konfrontiert sind. Hieraus können deutlich einfacher als aus quantitativen oder klassisch sozialwissenschaftlichen Verfahren Geschichten, Metaphern, Bilder, Emotionen u. v. m. abgeleitet werden, die sich dann produktiv innerhalb von Kommunikation nutzen lassen. Damit adressiert das Verfassungsmarketing anstelle von sich auflösenden Zielgruppen der Sozialforschung die Kommunikationsstrategien auf einer lebendigen, narrativen Ebene – und das lange, bevor das Marketing die aktuell trendigen Repräsentationen von Konsumenten, sogenannter „Personas“, „erfunden“ hat [15].
- **Tiefeninterview:** Beim psychologischen Tiefeninterview wird im Rahmen eines sich verdichtenden Kommunikationsprozesses so „tief gegraben“, bis die psychoLOGISCHE Wurzel eines Phänomens zu erkennen und zu beschreiben ist. Eine damit verbundene Darstellung gerät so breit und umfassend, wie es die jeweilige Fragestellung pragmatischer Weise erfordert. In den anderthalb- bis zweistündigen Einzelinterviews decken Psychologen und Psychologinnen bei Security-Wirkungsanalysen die unbewussten seelischen Wirkungen und Einflussfaktoren auf, die das Verhalten aller Personen in Verbindung mit Sicherheit bestimmen. Diese werden motiviert, in ihrer eigenen Sprache alles zu beschreiben, was ihnen im Zusammenhang mit ihrer Arbeit, ihrem generellem Wirken und der Informationssicherheit durch Kopf und Bauch geht. Statt quantitativer Meinungsumfrage ohne Möglichkeit auf Vertiefung einzelner Aspekte werden offene Interviews geführt, in denen auf Zusammenhänge zwischen Gesagtem, Körpersprache (wie Mimik, Gestik) und auch auf Fehlleistungen geachtet wird. Dabei werden die geheimen bzw. nicht bewusst wahrgenommenen Bedeutungszusammenhänge erforscht und nachvollziehbar gemacht. In einem derartigen Setting eröffnen sich somit stets neue Wendungen und oft überraschende Einblicke, die dann systematisch auf ihre Verhaltensrelevanz weiterverfolgt werden. Der hier zugrundeliegende Leitfaden ist ein „lernender Leitfaden“. D. h., in Tiefeninterviews überraschend auftretende Aspekte können ad hoc im Interview selbst und innerhalb nachfolgender Explorationen berücksichtigt werden. Damit liefern tiefenpsychologische Security-Studien intensive und wissenschaftlich abgesicherte Analysen auf Basis von kleinen, aber aussagekräftigen Stichproben. Hierbei reicht diese verhältnismäßig kleine Menge an Teilnehmenden aus, da die wirksamen Motivkomplexe und Einflussfaktoren in jedem Einzelinterview vollständig repräsentiert sind. Der Vorteil dieser Methode ist, dass alle verdeckten Security-Motive erfasst und in einen psychoLOGISCHen Kontext gestellt werden. Auf Basis dieser Ergebnisse können dann zielgenaue und konkrete Empfehlungen zur Verbesserung der Sicherheitskultur bzw. -maßnahmen eines jeden Unternehmens formuliert werden [14].

2.2 Auffälligkeiten in der Exploration

Die Rekrutierung für die anonymisierten Interviews und deren Durchführung erwies sich als schwieriger als ursprünglich angenommen:

- Die Vereinbarung gestaltete sich sehr zeitaufwendig, da z. B. Termine teilweise (mehrfach) abgesagt wurden und verschoben werden mussten.
- Die Sicherheitseinstellungen mancher von den Teilnehmenden verwendeten PCs oder Notebooks verhinderten eine adäquate Durchführung, da z. B. das eingeplante Testmaterial nicht per Live-Video evaluiert werden konnte.
- Einige Mitarbeitende wurden von den jeweiligen Geschäftsführungen zur Teilnahme beordert, teilweise ohne vorher deren Interesse bzw. Bereitschaft zu erfragen.

- Die Erwartungshaltung gegenüber dem Projekt hat sich in Einzelfällen als sehr hoch bzw. sehr agil („Ergebnisse am liebsten sofort“) herausgestellt.

Die geplanten Quotierungsvorgaben zu Geschlecht, Alter und den verschiedenen Funktionen bzw. Hierarchieebenen konnten aufgrund der mühevollen Akquise durch die beteiligten KMU teilweise nicht eingehalten werden:

- So wurden statt der 20 geplanten Online-Interviews lediglich 6 Frauen, aber 10 Männer befragt.
- Es wurde lediglich mit 2 Angestellten und 1 Auszubildenden gesprochen; die verbleibenden 13 Interviews wurden mit Führungskräften, (zukünftigen) Geschäftsführungen und deren Assistent/innen sowie den designierten IT-Fachleuten geführt.

Unbewusste Kontrolle von Mitarbeitenden

Die beiden Gespräche mit den Mitarbeitenden ohne Führungsfunktion fanden zudem im Unternehmen selbst und nicht im Homeoffice statt. Zu erwähnen ist, dass in einem Fall die Geschäftsführung das Interview kurz unterbrach. Es stellt sich daher die Frage, ob dies einen Einfluss auf den Gesprächsinhalt haben könnte.

Aus psychologischer Sicht stellen die schwierige Akquise mit der Anpassung der Stichprobe und der (unbewussten) Kontrolle der an den Interviews teilnehmenden Mitarbeitenden keine Zufälle dar. Vielmehr offenbaren sich dadurch relevante Hinweise auf wirksame Motive, die im Kontext des Themenkomplexes „Informationssicherheit und Mitarbeiter-Awareness“ schwer zu vereinbaren sind, etwa emotionale Ausbrüche (Hoffnungen, Befürchtungen etc.) und generell Paradoxes.

3. Informationssicherheit in kleinen und mittleren Unternehmen

Das Thema „Informationssicherheit“ ist unmittelbar verbunden mit den Besonderheiten von KMU. Die KMU werden dabei selbstbewusst in einem Spannungsfeld von familiärem, vertrauensvollem Miteinander und einem flexiblen Eingehen auf die Marktbedürfnisse präsentiert.

In allen Gesprächen werden die hohe Identifikation und Verbundenheit mit dem jeweiligen Unternehmen deutlich. Die Geschäftsführungen und auch die anderen Führungskräfte betonen die familiäre Zusammengehörigkeit, die Loyalität sowie das hohe Vertrauen in die Mitarbeitenden. Es wird Verständnis für die Nöte und Eigenheiten des jeweils anderen deutlich, und ein Bild des entspannten und meist harmonischen Miteinanders wird gezeichnet. Die Größe der Unternehmen ermöglicht zudem einen direkten Kontakt zu Mitarbeitenden. Die folgenden den Interviews entnommenen Zitate verdeutlichen die Situation in den ausgewählten KMU:

„Das ist bei uns ganz familiär.“

„Ich würde schon fast von einem harmonischen Miteinander sprechen.“

„Mir ist ein freundlicher, wertschätzender Umgang wichtig.“

„Das ist der Unterschied zu einem Großunternehmen: man kennt sich und vertraut sich.“

Dieses familiäre Miteinander zeigt sich auch in den Interviews selbst – die Teilnehmenden erlauben mitunter vertraute Einsichten in das eigene (Privat-)Leben:

- Zwar starten einige Gespräche mit offiziellen, Corporate Design-affinen Bildschirmhintergründen, diese werden jedoch trotz ausreichender Bandbreite bei der Übertragung schnell ausgeschaltet. Es wird deutlich, dass die Interviews infolge der Pandemie überwiegend aus Homeoffices geführt werden.
- Private Gegenstände beleben die Hintergründe.
- Nach einer distanzierten Aufwärmphase machen sich die Teilnehmenden locker und involvierten die Interviewer/innen nebenbei in private Details.

Zugleich wird das jeweilige Unternehmen als kompetent (und erfolgreich auf dem Markt agierend) präsentiert. Die eigenen Aufgaben im Unternehmen werden stolz dargestellt und die teils komplizierten Abläufe geduldig erläutert. Gerade die hohe Flexibilität, das Finden von individuellen Lösungen und die schnellen Reaktionen auf Marktbedürfnisse zeichnen die KMU aus. Diese Agilität hat sich in Zeiten der Pandemie bewährt, in denen das Arbeiten im Homeoffice nicht nur erlaubt, sondern durch die zügige Bereitstellung von Equipment (Laptops, Headsets, Kameras etc.) unterstützt wurde. Dies ist auch der folgenden Äußerung einer interviewten Person zu entnehmen:

„Das war schon beeindruckend: innerhalb von kürzester Zeit waren 80 Laptops da und die Kollegen und Kolleginnen konnten von zu Hause arbeiten. Das hat unsere IT wirklich gut gemacht.“

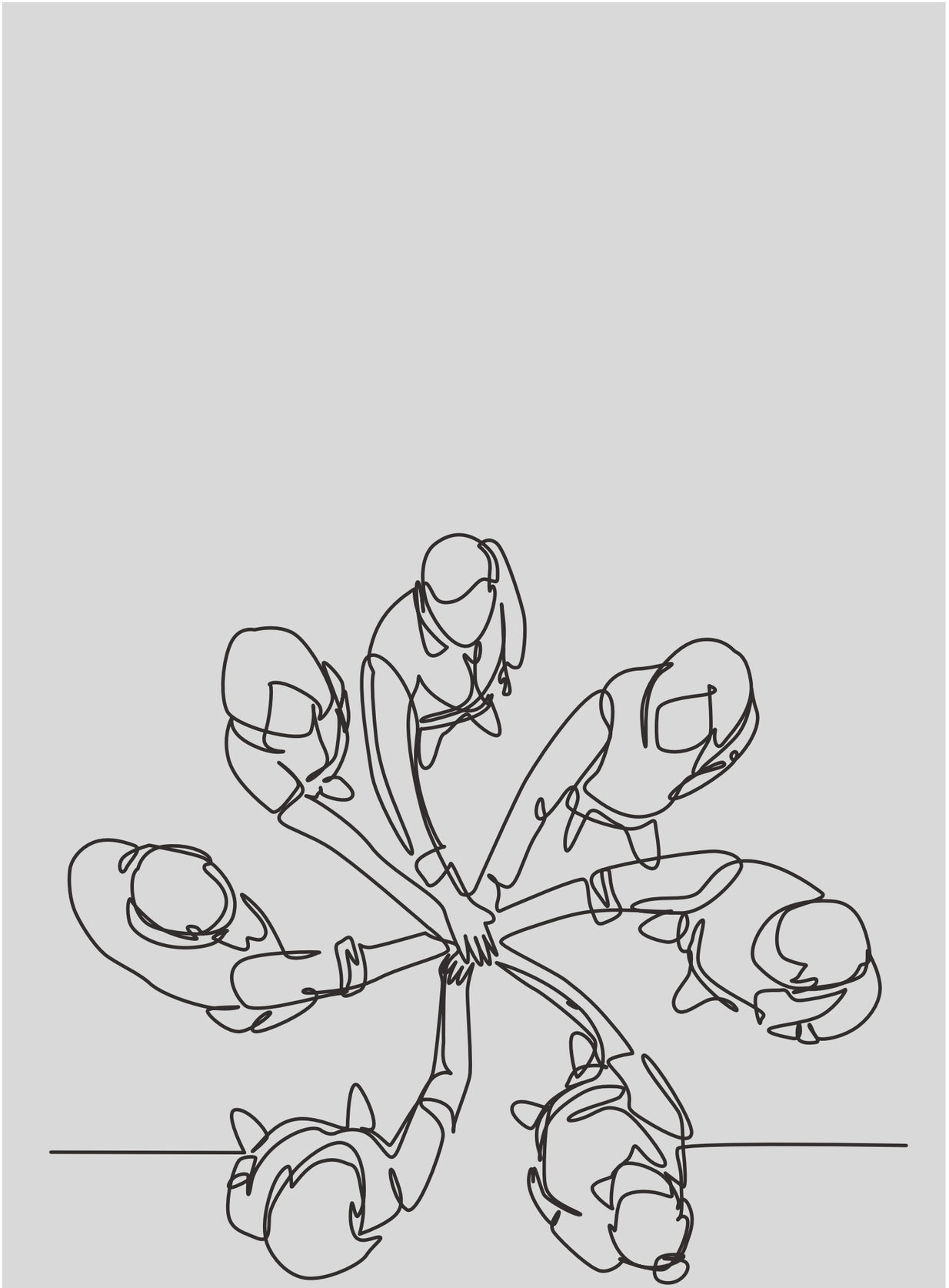
3.1 Exkurs: Tätigkeits-, Sicherheits- und Kompetenzprofile sowie daraus resultierende Themen

In allen Branchen und Tätigkeitsbereichen ist die Verarbeitung von Daten bzw. die Nutzung digitaler Kommunikation essenziell. In den KMU gibt es unterschiedliche Tätigkeitsprofile (offizielle, vom Arbeitgeber veranlasste Beschreibungen der mit einer Tätigkeit verbundenen Aufgaben bzw. Erwartungen) mit differenzierten und individuellen Sicherheitsprofilen (Addition von sicherheitsrelevanten Skills sowie Zutritts- bzw. Zugriffsrechten) und Kompetenzprofilen (Gesamtheit aller Fähigkeiten auch der impliziten, nicht in Tätigkeitsprofilen beschriebenen) sowie Rollen, die mehr oder weniger mit sensiblen Informationen und den verschiedenen Informationssicherheits- bzw. Datenschutzrisiken in Kontakt geraten.

Aufgrund der Heterogenität der Stichprobe konnte hinsichtlich der Diversifikation von Tätigkeits-, Sicherheits- und Kompetenzprofilen für den Bereich „Security Awareness“ in KMU keine unmittelbare psychologische Relevanz ermittelt werden.

Über alle Unterschiede hinweg existieren allgemeingültige Risiken bzw. Sicherheitsthemen, die quer durch alle Bereiche, Verfassungen und Zielgruppen benannt werden und im Arbeitsalltag für alle der befragten Personengruppen eine wesentliche Rolle spielen. Zu diesen zählen z. B.:

- Authentifizierung, Umgang mit (komplexen) Passwörtern
- Identifizierung von bzw. Umgang mit Phishing-Mails bzw. Angriffen, basierend auf Phishing und ähnlichen Angriffsprinzipien
- Sichere Verschlüsselung von E-Mails bzw. Dateianhängen



3.2 Sicherheitsrelevante Besonderheiten in der Kommunikation

Neben „E-Mail“ spielt in den KMU in Bezug auf Kommunikationskanäle das Thema „Messenger“ eine große und immer stärker werdende Rolle.

Dabei wird die Nutzung von Messenger sehr unterschiedlich gehandhabt: In einigen Unternehmen und Unternehmensbereichen wird WhatsApp kritisch betrachtet, in anderen wiederum verlangen relevante Kunden nach einem geschäftlichen Kontakt über WhatsApp und verschicken mitunter sensible Daten über diesen Kanal.

Folgende Zitate stammen aus den geführten Interviews und bestätigen diese Aussagen:

„Es gibt Kunden, die bestellen ausschließlich per WhatsApp, also sagen die Kollegen: entweder machen wir Geschäft oder wir machen keins. Da kann ich noch so erklären, wie gefährlich WhatsApp ist. Das ist dann egal.“

„Wir haben auch eine Firmengruppe in WhatsApp. Teilweise bin ich schon erstaunt, was die Leute da posten. Also Kinderbilder sind für mich tabu – aber das muss jeder selber wissen. Ich selber bin da wenig aktiv, schaue aber schon da rein.“

Alternative Messenger sind weder bekannt noch werden diese im Unternehmenskontext genutzt.

In den befragten KMU wird oftmals „Microsoft Teams“ eingesetzt, um in Pandemiezeiten einen weiterhin engen Kontakt zu den Mitarbeitenden und vor allem einen reibungslosen Arbeitsalltag aufrechtzuerhalten.

Sehr klar wird benannt, dass dem „komfortablen Handling“ Vorrang vor möglichen Sicherheitsaspekten gegeben wird. Dies wird von der IT-Administration in den Unternehmen nicht immer positiv gesehen.

„Wir haben jetzt Teams. Für die Entscheidung war uns wichtig, dass das mit dem ganzen Office-Paket kompatibel ist. Das muss einfach reibungslos funktionieren und das tut es auch.“

„Wir haben jetzt die Testversion mit 10 Mitarbeitern getestet. Für uns ist es wichtig, dass es nicht kompliziert ist.“

Generell steht die im Rahmen der Online-Interviews erlebte, sehr restriktive Haltung bezüglich Videokonferenz-Tools im Widerspruch zum lockeren Umgang mit Messengern – vor allem bei der Kommunikation mit Kunden.

3.3 Sicherheitskultur in KMU

Dem Thema „Sicherheit“ wird auch hinsichtlich des eigenen Geschäftserfolgs eine hohe Bedeutung zugeschrieben: Geschäftsführungen, Führungskräfte, IT-Administration wie auch weitere Mitarbeitende bekräftigen die Relevanz des Themas und betonen eigene Anstrengungen und den erreichten Schutz durch die bereits erfolgten Maßnahmen. Das eigene Unternehmen erscheint dabei als „Festung“, die selbstbewusst den Gefahren „von außen“ trotzt, wie folgende Interviewauszüge zeigen:

„Wir sind Fort Knox.“

„Das wissen alle, wir sind da schon gut aufgestellt.“

„Sicherheit ist wichtig!“

Auf den ersten Blick umfasst der Bereich der Informationssicherheit die technischen Schutzmaßnahmen (Firewall, Netzwerksicherheit, eigene Server vs. Cloudlösungen, Hard- und Software) sowie den Datenschutz mit Verweis auf die Datenschutz-Grundverordnung sowie Compliance mit den internen Richtlinien. Hinsichtlich der zentralen Informationssicherheitsrisiken werden vor allem „Hackerangriffe“ und generell Cyber-Kriminalität mit der steigenden Anzahl von E-Mails mit „bösartigem Anhang“ bzw. Links benannt.

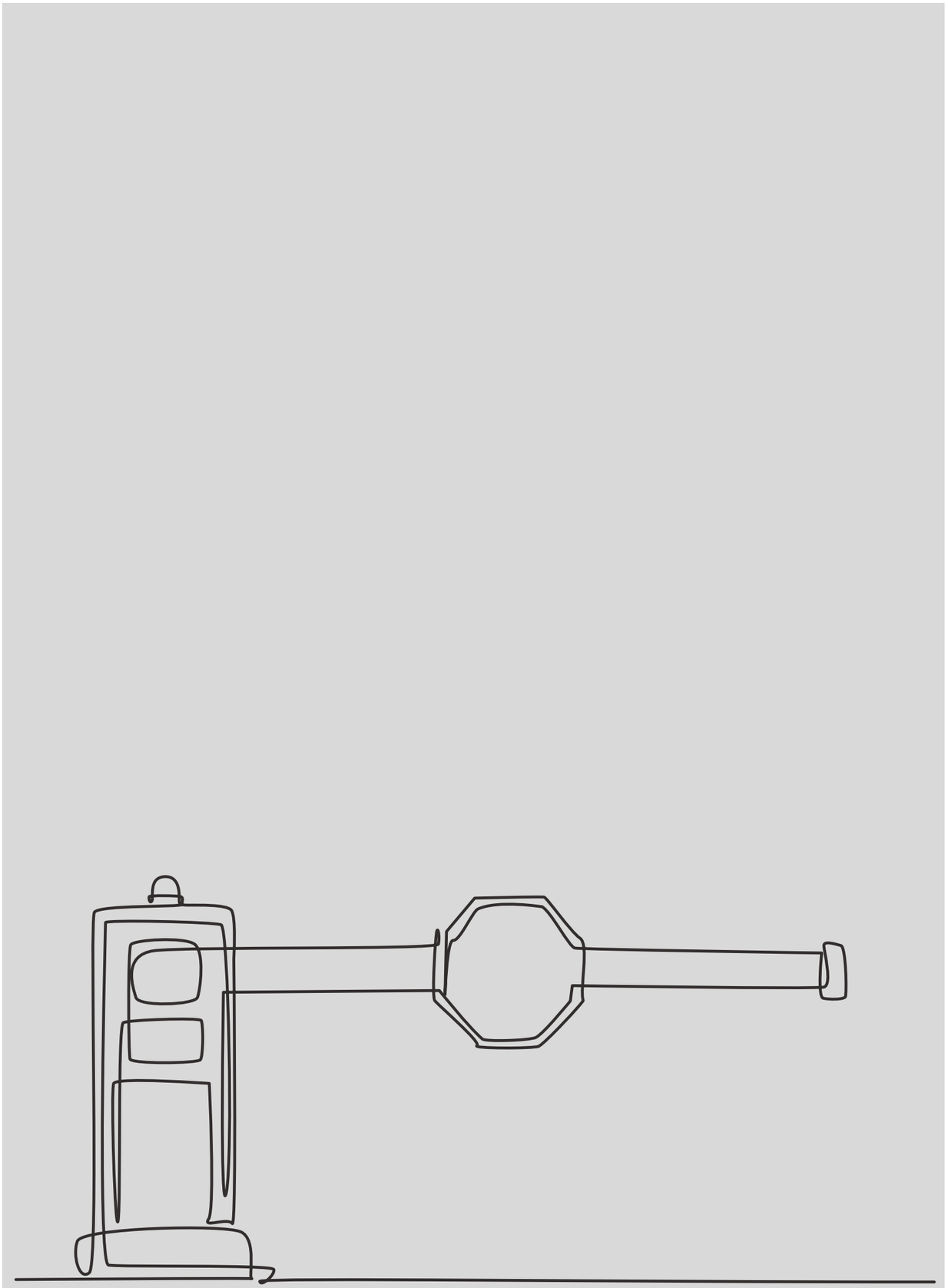
Nicht nur die Gefahren für das Unternehmen werden als von außen kommend gesehen. Auch der Schutz selbst wird in den Pilotunternehmen oftmals an externe Datenschutzbeauftragte, IT-Dienstleister oder IT-Support delegiert. Intern werden dann IT-Administration oder Datenschutzkoordinatoren/innen eingesetzt. In einigen Fällen übernehmen kompetente Kollegen/Kolleginnen auf Zuruf die Aufgabe, die laut einer der interviewten Personen „den Bereich dann nebenher mitmachen“. Die im Folgenden aufgezählten Kommentare aus den Interviews belegen diese Perspektive:

„Durch die Cloud sind wir autark. Das lässt mich ruhig schlafen. Da muss ich mich auf die Anbieter verlassen. Microsoft hat da ganz andere Möglichkeiten als wir.“

„Wir haben eine große interne Serverlandschaft plus externem Datenschutzbeauftragten.“

„Wir nutzen den Newsletter des BSI.“

„Unsere externen Dienstleister sind manchmal auch am Wochenende vor Ort, sodass es selten einen persönlichen Kontakt gibt … eher telefonisch, wenn nötig.“



3.4 Security Awareness in KMU

Die Interviews bestätigen, dass in allen der beteiligten KMU Schulungen oder andere Sensibilisierungsmaßnahmen stattfinden:

> *„Es gibt regelmäßig Meetings und E-Mails zu dem Thema. Aber ich weiß nicht, in welchem Turnus. Generell werden neue Mitarbeiter zum Thema ‚IT-Security' eingewiesen, und dann gibt es Unterweisungen als Auffrischung."*
>
> *„Vor Corona hatten wir regelmäßige Meetings, da war auch immer mal ein Sicherheitsthema dabei."*
>
> *„Bei Bedarf bekommen die [Mitarbeiter] Mails und es wird gefragt: Ist das Phishing?"*
>
> *„So zweimal im Jahr haben wir Sicherheitsthemen."*

Ungestützt wird das Thema „Informationssicherheit", gerade im Kontext von Awareness, schnell mit dem Thema „Datenschutz" wie auch in einer ganzheitlichen Perspektive von Sicherheit mit den Themen „Compliance", „Arbeits-" oder „Brandschutz" verbunden. Dabei umfasst das Thema „Sensibilisierung" in Bezug auf Datenschutz zentral jene im Interview benannten, sensiblen Daten, die es zu schützen gilt:

- „Personenbezogene Daten"
- „Sensible Themen, etwa Gehalt"
- „Verträge", „Vertragsdetails"
- „Firmengeheimnisse"

> *„Informationssicherheit ist für mich: das Bewusstsein zu schärfen für die bösen Menschen, die einem Viren schicken wollen, und wohin die Daten dann kommen."*

Analog dazu werden oft technische „Einweisungen" oder die so genannten „jährlichen Auffrischungen" als erinnerte Sensibilisierungsmaßnahmen zur Verbesserung der Informationssicherheit benannt.

Eigene Gesundheit und die des Unternehmens sind in Zeiten der Pandemie wichtiger als die Informationssicherheit

In manchen KMU werden derartige Unterweisungen (z. B. auf Grundlage der DSGVO) auch als jährliche „Update-Meetings" abgehalten. Andere KMU behandeln Sicherheitsthemen in wöchentlichen Meetings oder Führungskräfte sprechen diese en passant in der Kaffeeküche (bzw. anders über den Kanal Flurfunk) an.

Während der Pandemie sind Informationssicherheitsthemen jedoch in den Hintergrund geraten und werden häufig dominiert von (der eigenen) Gesundheitsprävention oder der (ökonomischen) „Gesundheit" des eigenen Unternehmens bzw. der eigenen Branche.

Der Begriff „Security Awareness" ist – anders als der der „Sensibilisierung" – entweder völlig unbekannt bzw. wenig präsent oder er kann nur gestützt erklärt werden. Verbunden wird damit dann ein umfassender, ganzheitlicher Umgang mit dem Thema „Sicherheit". Als Beispiel wird unter anderem benannt, dass z. B. als Protagonisten von Awareness engagierte „Kümmerer" im Sinne von „Sicherheitssozialarbeitern" gemeint wären, denen ihr „Security Streetworking" mit einer vorwiegend persönlich geleiteten Ansprache von Kollegen und Kolleginnen mindestens genauso wichtig erscheint wie etwa das technische Dichtmachen der eigenen Organisation.

> *„Das klingt seriös, da habe ich das Gefühl von was Gutem, von Unterstützung – dass ich an die Hand genommen werde, um die Sicherheit zu mehren."*
>
> *„Damit verbinde ich, dass man das Sicherheitsbewusstsein schärfen muss. Das geht nur über Drills, immer wieder. Mission Awareness gegen Missing Awareness, wenn Sie so wollen."*

Ganzheitliche Security Awareness-Konzepte, wie im Projekt „Awareness Labor KMU (ALARM) Informationssicherheit" vorgesehen, oder ein Awareness Framework mit dokumentierter Strategie kommen bisher in den befragten KMU ebenso wenig zum Einsatz wie Security Awareness-Messungen oder andere Evaluationen im Kontext der Sensibilisierung von Mitarbeitenden.

Die befragten KMU beschränken sich hinsichtlich Awareness vor allem auf die Lerntheorie (Ebene 1: Wissensvermittlung, s. S. 15), ergänzt um systemisch-diskursive Settings (Ebene 3, s. S. 15), die allerdings eher intuitiv-beiläufig erfolgen und abgetrennt sind von der Ebene der Wissensvermittlung. Security Marketing (Ebene 2, s. S. 15) als eine Art „Mittelbau" der hier zugrunde gelegten Security Awarenss-Methodik (s. S. 15-17) fehlt völlig – verständlich angesichts der in KMU verfügbaren Mittel. Offenbar führt vor allem fehlende Verbindung der einzelnen Awareness-Ebenen zu eingeschränkten, manchmal zu lediglich zufälligen Sensibilisierungserfolgen.

3.5 Incident Management und Reportingkultur

Der Umgang mit konkreten oder vermeintlichen Sicherheitsvorfällen unterstützt das präsentierte Bild der „wehrhaften KMU" in ihrem „Kampf" gegen von außen kommende Gefahren. Durch einen Sicherheitsvorfall wird die Bindung gar gestärkt:

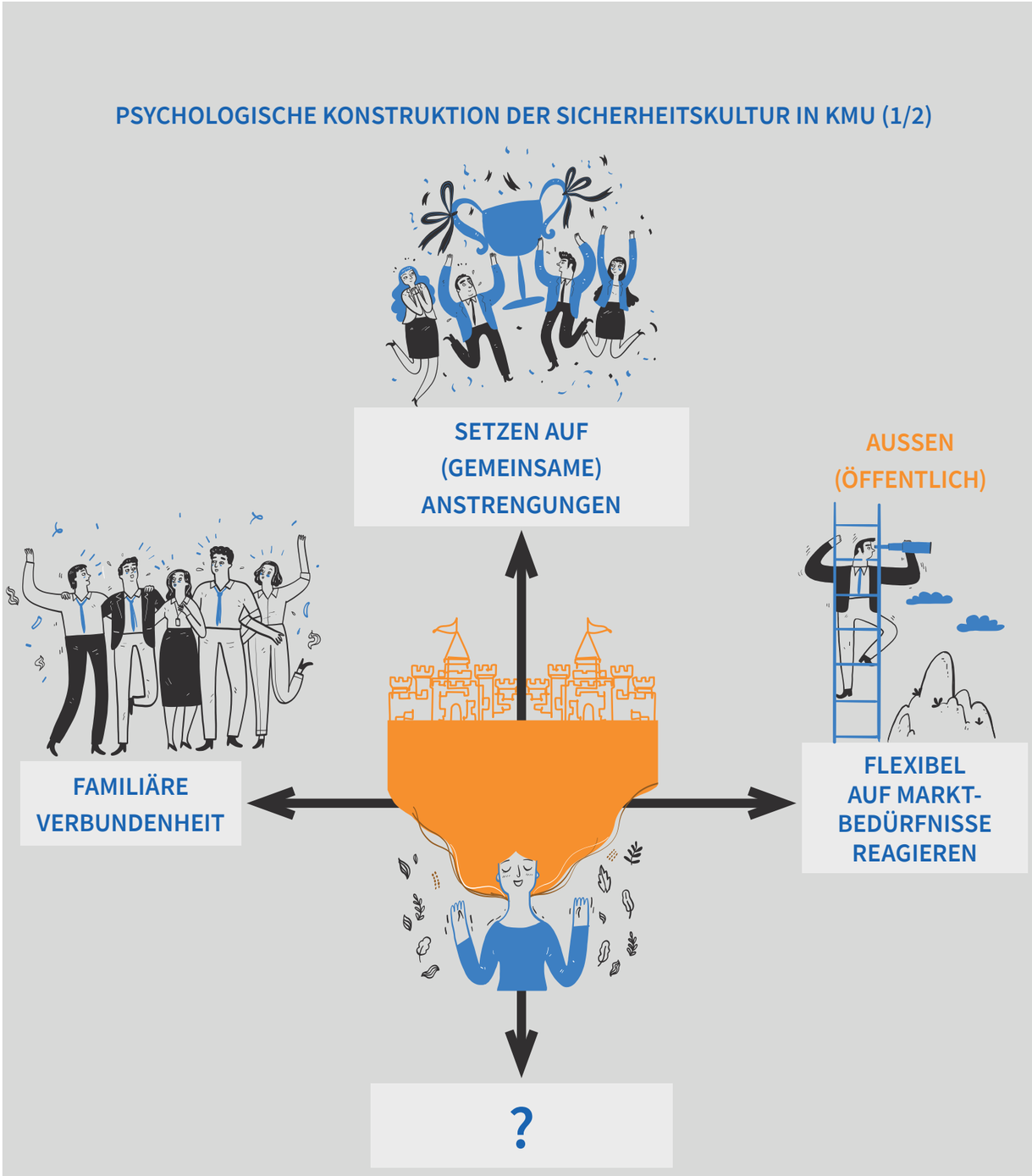


Abb. 1: *Psychologische Konstruktion ohne Kehrseite (?)*

- Die jeweiligen Meldewege sind bekannt. Zu den konkreten Ansprechpartnern besteht in der Regel ein persönliches, vertrauensvolles Verhältnis. Auch das „Bauchgefühl" der Mitarbeitenden wird respektiert.
- CEO-Fraud-Versuche werden als scheiternde Versuche dargestellt, da der Kontakt zur Geschäftsführung oder der IT-Administration von den potenziellen Opfern offenbar ohne Zögern aufgenommen und somit Betrug relativ schnell sichtbar gemacht werden kann.

Nachfragen sind scheinbar jederzeit möglich: „Die IT hat stets ein offenes Ohr und eine gute Antwort."

- Jeder noch so kleine Sicherheitsvorfall wird potenziell schnell bekannt und führt ohne viel Aufwand vermeintlich zu erhöhter Wachsamkeit bei den anderen.
- Durch die zum Teil jahrelange Verbundenheit der Teilnehmenden zum Unternehmen bestehen keinerlei Bedenken, eigene Fehler zuzugeben. Keiner der Befragten muss negative Konsequenzen fürchten, wenn ein Fehler offenbart wird.

Eine derartig positive Darstellung von Sicherheitskommunikation bzw. Fehlerkultur bei den befragten KMU erscheint bemerkenswert und insgesamt deutlich positiver als in anderen, vergleichbaren Studien beschrieben (z. B. „Studie zur Information Security Awareness in kleinen und mittleren Unternehmen" [16] oder „Aktuelle Lage der IT-Sicherheit in KMU" [17]). Diese werfen u. a. die Frage auf, welche produktive Leistung die befragten Unternehmen von einer Optimierung ihrer Security Awareness durch die Beteiligung an dem Projekt noch erwarten dürfen.

3.6 Psychologische Konstruktion der Sicherheitskultur in KMU

Der vermeintlich offene Umgang mit Sicherheitsvorfällen und die positive Fehlerkultur werden vor allem von den einfachen Angestellten und Assistent/innen betont und geschätzt:

„Egal, was man gemacht hat: Da passiert nichts."

„Der muss dann höchstens einen Kuchen backen, wenn er das dritte Mal den Rechner nicht gesperrt hat."

„Wir haben eine No-Blame-Kultur."

Das Nichtbeachten von Regeln führt zu keinen Konsequenzen

Sicherheitskultur in KMU stellt sich dann so wie in der Abbildung 1 (links) dar. Zugleich zeigt sich in der KMU-Fehlerkultur eine ungünstige Kehrseite der familiären Verbundenheit: Das Nichtbeachten von Regeln führt offenbar zu keinerlei Konsequenzen. Selbst wenn Regeln bekannt sind und deren Einhaltung eingefordert wird, bleiben negative Konsequenzen bei Fehlverhalten weitgehend aus. Dies führt zu Unmut in der IT-Administration, bei Assistent/innen und den übrigen Angestellten:

„Wir sollen den Bildschirm sperren. Das macht aber keiner. Wenn es um Kundendaten geht, sagt auch keiner was. Aber wehe, wenn es sich um eine Datei mit Personaldaten handelt, da ist dann was los!"

„Wir haben einen Außendienstler, den kümmert das nicht. Der weigert sich, regelmäßig Updates aufzuspielen. Der weiß, dass er uns alle gefährdet, aber der macht 12 Millionen Umsatz im Jahr. Der erfährt keine Konsequenzen."

Bei weiterer Vertiefung werden bislang verborgen gehaltene Seiten deutlich: Die einzelnen Unternehmensbereiche äußern sich dann kritisch über die jeweils anderen.

Risiken nicht nur von außen

Es wird offenbart, dass Gefahren nicht allein außerhalb des jeweiligen KMU liegen. Deutlicher als in einem Großunternehmen treten die Gefahren aus dem Inneren zu Tage, die durch die Nähe und Vertrautheit im Unternehmen und die Forderung nach flexibler Kundenorientierung zusätzlich gefördert werden. Dies wurde wie folgt kommentiert:

„Ich kann das Gerede der Digital Natives nicht mehr hören. Die wollen bei uns IT-Systemadministratoren werden, sind aber nicht mal in der Lage, eine Excel zu erstellen. Da können Sie ganz von vorn anfangen mit dem Thema ‚Datenschutz'"

„Man mag es kaum sagen, aber ich könnte Ihnen sofort einige Mitarbeitende aufzählen, die für alles nur ein Passwort haben – und die sitzen nicht nur an unwichtigen Stellen."

„Ich höre dann oft: ‚Ich verstehe es ja, aber der Aufwand!'"

„Der Vertrieb sitzt schon zwischen den Stühlen. Man kann den Kunden auch nicht belehren."

„Ganz klar: Das ist für die meisten doch nur nervig und behindert den eigenen Workflow."

„Auf einer Skala von 0 bis 10 sind wir bei 5 bis 6."

PSYCHOLOGISCHE KONSTRUKTION DER SICHERHEITSKULTUR IN KMU (2/2)

SETZEN AUF (GEMEINSAME) ANSTRENGUNGEN

AUSSEN (ÖFFENTLICH)

FAMILIÄRE VERBUNDENHEIT

FLEXIBEL AUF MARKT-BEDÜRFNISSE REAGIEREN

INNEN (VERBORGEN)

IN VERSTRICKUNGEN GEFANGEN

Abb. 2: *Psychologische Konstruktion inklusive Kehrseite*

> *„Das ist einfach nervig! Bestimmte Dateien landen in Quarantäne, man muss ein Ticket ordern, um bestimmte Mails freizubekommen. Das dauert. Aber Safety first!“*
>
> *„Am liebsten würde ich gar keine Sicherheits-freigaben machen. Aber dann schreien die.“*
>
> *„Ganz ehrlich, wir arbeiten oft in der Grauzone. Man weiß, dass es eigentlich nicht geht. Aber solange nichts passiert, sagt keiner was. In 95 % der Fälle geht es gut, bei den 5 % ist dann Gejaule.“*
>
> *„Sicherheit ist wichtig. OK. Wir entwickeln ja auch selber. Das wissen alle, dass das wichtig ist. Aber dann heißt es: ‚Ja, aber die anderen dürfen‘ und es wird schwierig.“*

Klare Regelwerke jenseits von (gesetzlichen) Standards, die Halt und Orientierung geben könnten, werden von den meisten vermisst und können von den Geschäftsführerenden teils nur rudimentär wiedergegeben werden. Die Ausnahme bildete ein befragter Geschäftsführer, der sehr klar ausführt:

> *„Am Regelwerk habe ich lange gefeilt […]. Es ist seit dem März in Kraft und wird als Datei hinterlegt, in Meetings vermittelt und als PDF in E-Mails von oben verteilt mit einer Frist für eine Rückmeldung, dass man es gelesen und verstanden hat. Dann haben wir die Unterschrift als Nachweis.“*

Befragte Mitarbeitende der Unternehmen berichten:

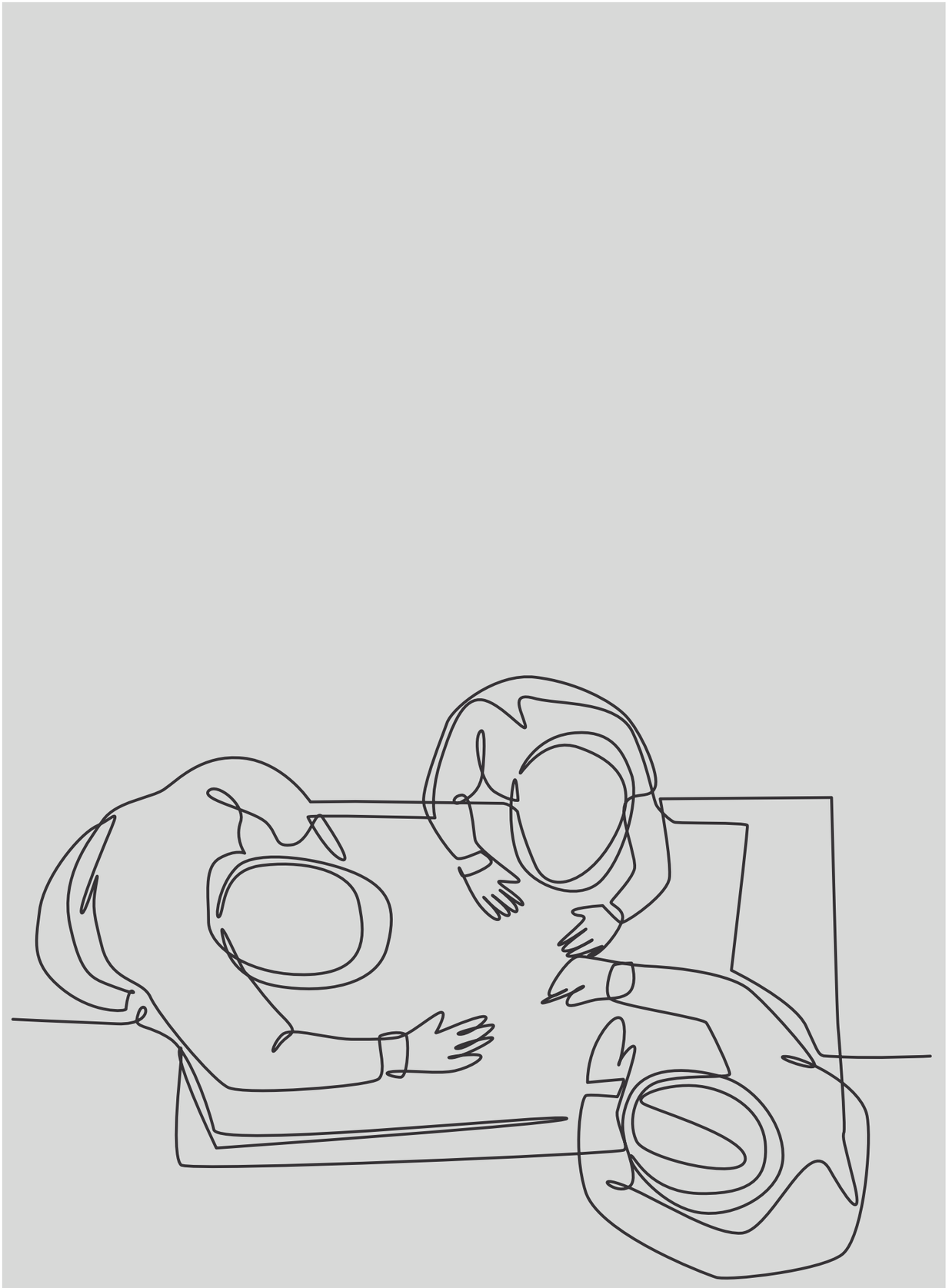
> *„Wir haben Regeln, aber ich wüsste nicht, wo.“*
>
> *„Ne, es gibt die DSGVO, aber sonst wüsste ich nicht“.*
>
> *„Im Intranet haben wir eine Spalte mit Datenschutz-regeln. Die habe ich aber noch nicht gelesen.“*
>
> *„Die Regeln sind schriftlich fixiert: Notebook zuklappen, Passwort-Manager benutzen.“*
>
> *„Wir haben die klare Regel: Personenbezogene Daten nie unverschlüsselt [verschicken]. Aber wir haben auch Kollegen, die schicken das PDF-Passwort in der gleichen Mail wie die PDF auch.“*

Bei konkreten Fragen zu den im Unternehmen durchgeführten Schulungsmaßnahmen wird deutlich: die Mitarbeitenden erkennen weder einen konkreten Plan, noch ist der Nutzen der Maßnahme stets offensichtlich. Eine systematische Sensibilisierung, die eine tatsächliche Sicherheitskultur entwickeln könnte, fehlt:

> *„Der externe Datenschutzbeauftragte war vor zwei Jahren da für drei, vier Stunden. Und die neuen Kollegen erhalten immer eine Einführung.“*
>
> *„Bei der letzten Auffrischung war ich nicht dabei. Und dieses Jahr ist die wegen Corona ausgefallen. Hm. Dann war das also vor drei Jahren das letzte Mal.“*
>
> *„Wir werden mit dem Kaspersky-Awareness-Tool Set geschult. Das sind mitunter zähe Themen. Das fällt selbst den IT-Profis schwer. Oft sind das Power-Point-Schlachten […] Das letzte Thema? Weiß ich gar nicht mehr.“*
>
> *„Wir haben keine [Sicherheitskultur], also nichts Aktives oder Regelmäßiges, sondern fallbezogen. Man unterhält sich mit der IT und erfährt dabei Sachen, wo man denkt: ‚Hoppla‘.“*

Durch die Auseinandersetzung mit dem Thema im Rahmen der Interviews wird den Teilnehmenden bewusst, dass die bisherigen Maßnahmen im Unternehmen nicht ausreichen. Die zuvor als positives Merkmal hervorgehobenen eigenen Anstrengungen zeigen sich in den Interviews angesichts der immer stärker in den Blick genommenen Gefahren als individuelle Überforderungen und Verstrickungen wie z. B. Schatten-IT (IT-Systeme bzw. -Prozesse, die sich neben der offiziellen IT-Infrastruktur etabliert haben). Die hierzu passende psychologische Konstruktion ist in der Abbildung 2 auf der linken Seite visualisiert.

> *„Ich habe da Nachholbedarf bezüglich meiner Mails bei der Arbeit. Die haben oft Viren und die entwickeln sich immer weiter. Da muss ich dranbleiben, um ‚sensibilisiert‘ zu werden.“*
>
> *„Wenn man sich das genau anschaut: Katastrophe!“*
>
> *„Soll ich da jetzt ehrlich darauf antworten? Sie kennen doch das Sprichwort vom Schuster und den Schuhen.“*
>
> *„Ob der ganze Aufwand was bringt? Die Änderungsbereitschaft einiger Kollegen ist doch sehr gering. Ob man die daher mit einer Maßnahme – so gut sie auch gemacht ist – erreicht, ist aus meiner Sicht mehr als fraglich.“*
>
> *„Es ist noch nicht ganz drin, dass man immer aufpassen muss. Deshalb sind reale Beispiele, wo man sich anschließend schlecht fühlt, nötig. Obwohl manche das unhöflich finden.“*



4. Rolle und Funktion der beteiligten Akteure mit Typologie

Auf Basis der evaluierten z. T. unbewussten Umgangsformen der Teilnehmenden mit dem Thema „Informationssicherheit“ lässt sich eine Typologie mit fünf prototypischen Strategien entwickeln.

Diese Einteilung ist stark vergröbert und generalisiert. Sie dient dennoch der Einschätzung von Schwachstellen und Bedarf in den Unternehmen.

4.1 IT-Kapitän/in

Dieser Typus sieht sich in einer Vorbildfunktion im Hinblick auf Informationssicherheit. Er/sie genießt es, voranzugehen, indem er/sie die aus seiner/ihrer Sicht sinnvollen Regeln einhält und dies auch kommuniziert.

Ihm/ihr ist gewahr, dass er/sie sich nicht immer beliebt macht, dies nimmt er/sie aber in Kauf im Gefühl, das Richtige zu tun und dafür auch einen gewissen Respekt zu ernten.

- **Positiv:** Das Vorbild und Mahnungen können andere Mitarbeitende sanft überzeugen, sich ebenfalls sicher zu verhalten.
- **Negativ:** Es besteht die Gefahr der Resignation und der (inneren) Kündigung, wenn die erhoffte Anerkennung ausbleibt.
- **Motto:** „Ich muss nicht von allen geliebt werden.“
- **Awareness-Kompatibilität:** Sensibilisierungsmaßnahmen können eine Chance sein, ihn/sie über die Bestätigung des eigenen Verhaltens hinsichtlich Informationssicherheit und den Gemeinschaftssinn zu motivieren und eine Resignation zu verhindern.

4.2 Vorfall-Experte/-Expertin

Dieser Typus findet sich meist in der IT-Abteilung und wird gerufen, wenn Not am Mann/an der Frau ist und der externe Service nicht erreicht wird.

Die Rolle beschränkt sich jedoch nur auf das Lösen von Schwierigkeiten – Erklärungen und Belehrungen werden von den Mitarbeitenden indes nicht gewünscht.

- **Positiv:** hohes Know-how, wird als Teil des Teams erlebt.
- **Negativ:** Die Kollegen und Kolleginnen können weiter in ihrer erlernten Sorglosigkeit festhalten.
- **Motto:** „Rettung naht.“
- **Awareness-Kompatibilität:** Sensibilisierungsmaßnahmen werden abgelehnt; sie untergraben seine/ihre Expertise.

4.3 Verständnisvoller Tröster/ Verständnisvolle Trösterin

Dieser (Führungskräfte-)Typus gibt vor, „seine Pappenheimer zu kennen“, wobei das gute kollegiale Miteinander und die Kundenorientierung klar im Vordergrund stehen.

Sicherheitsverstöße werden zwar wahrgenommen, aber meist ignoriert oder gar in Abwägung gebilligt. Es wird eben Trost gespendet – was die eigene Sicherheits-Messlatte weiterhin senkt.

- **Positiv:** Fördert die gute Arbeitsatmosphäre und verfestigt eine auf Verständnis basierende Fehlerkultur.
- **Negativ:** Trägt nicht zur Erhöhung des Sicherheitsniveaus bei.
- **Motto:** „Wir sind eine große Familie.“
- **Awareness-Kompatibilität:** Sensibilisierungsmaßnahmen stärken seine/ihre Positionierung.

4.4 IT-Notfallsirene

Dieser Typus stört sich am sorglosen Verhalten seiner Kolleginnen und Kollegen, Vorgesetzten und Kunden. Der direkte Hinweis auf Fehler hat sich jedoch als unzureichend erwiesen, er erfährt kaum Rückendeckung, was zu einer hohen Frustration führt.

Bei Gleichgesinnten brechen der Ärger und das Unverständnis mitunter hervor. Wird das Fehlverhalten der anderen gar dem Vorgesetzten gemeldet, führt das zu sozialem Unfrieden.

- **Positiv:** Hohes Interesse an Sicherheitsthemen und gute Kenntnis von Gesetzen bzw. internen Sicherheitsregeln.
- **Negativ:** Macht sich schnell unbeliebt und läuft Gefahr, aus der KMU-Familie ausgestoßen zu werden.
- **Motto:** „Einer muss es tun.”
- **Awareness-Kompatibilität:** Sensibilisierungsmaßnahmen der Informationssicherheit taugen als Beleg ihrer ständigen Mahnungen; sie tragen zu mehr Glaubwürdigkeit und Bindung bei.

Abb. 3: *Typologie der beteiligten Akteure*

4.5 Volldelegierer/in

Dieser Typus verlässt sich beinahe komplett auf die Security-Profis bzw. die IT-Administration. Mit Sicherheit hat er/sie nichts am Hut. Er/sie hat das Gefühl, eh nichts beitragen zu können, da er/sie denjenigen Profis vertraut, die Schutzmaßnahmen als rein technische Angelegenheit verstehen.

- **Positiv:** Trägt durch seine/ihre naive Offenheit zur Sichtbarkeit von Sicherheitslücken bei.
- **Negativ:** Demonstrative Sorglosigkeit provoziert Ärger.
- **Motto:** „Um Informationssicherheit sollen sich die Experten kümmern."
- **Awareness-Kompatibilität:** Sensibilisierungsmaßnahmen zwingen ihn/sie zu einer Positionierung; er/sie muss sich entscheiden, ob er/sie doch Verantwortung annimmt oder nicht.

Sämtliche Typen existieren nicht in der hier plakativ dargestellten Reinform, sondern in der Regel als Durchmischung, z. B. 40-30-20-10-0 (prozentuale Anteile an jedem Prototypen). Der Arbeitsalltag der Teilnehmenden ist also durch eine Konstellation verschiedener Strategien im Umgang mit dem Thema „Informationssicherheit" geprägt, die wiederum von den unterschiedlichen psychologischen Verfassungen bestimmt sind. Aus der Typologie können metaphorisch verschiedene Security-Gesichter eines KMU-Mitarbeitenden abgeleitet werden.

Alle anderen Typen können mithilfe von Awareness-Maßnahmen nur gewinnen und ihre jeweiligen Positionierungen verbessern, wenn sie aktiv und involviert an Maßnahmen teilnehmen oder als Multiplikator/in bzw. Botschafter/in sogar mithelfen, diese zu bewerben, zu moderieren bzw. durchzuführen.

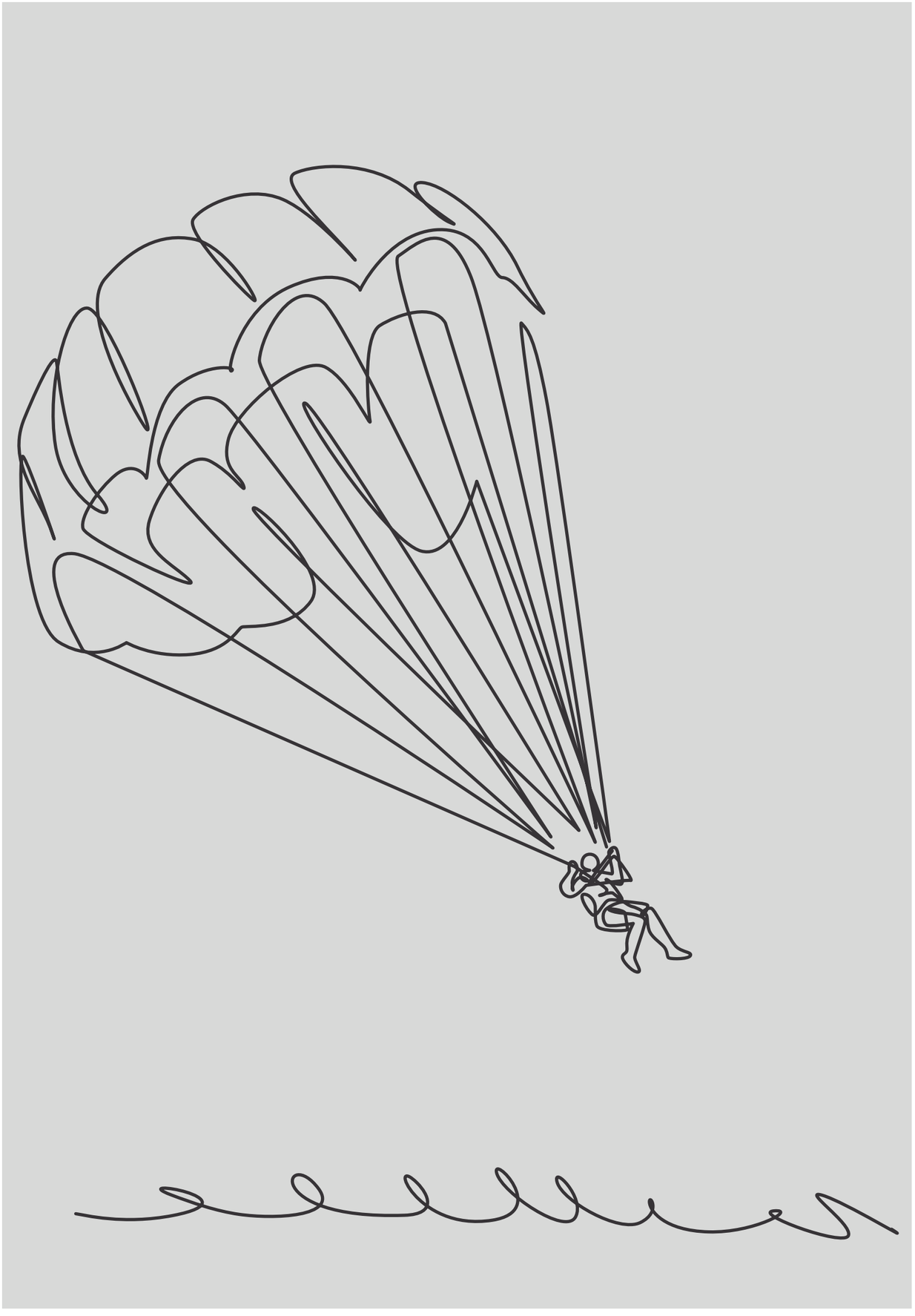
Alle Typen würden von Awareness-Maßnahmen profitieren – manche mehr – manche weniger.

In Bezug auf die Kompatibilität zu Awareness-Maßnahmen kann nicht jedem Typus Offenheit zugestanden werden. Es existiert allerdings kein Tabu-Typus, bei dem mit völliger Reaktanz zu rechnen wäre.

Am schwierigsten werden der/die IT-Kapitän/in und der/die Vorfall-Experte/-Expertin in Maßnahmen zu involvieren sein.

Der/die IT-Kapitän/in benötigt vor allem Anerkennung und der/die Vorfall-Expert/-Expertin hat als fleischgewordener „Security-Booster" potenziell am meisten zu verlieren. Daher wird es bei dem/der IT-Kapitän/in darauf ankommen, ihn/sie als Multiplikator/in bzw. Botschafter/in von Awareness-Maßnahmen zu positionieren.

Für den/die Vorfall-Experten/in ist wiederum wichtig, neben Awareness-Maßnahmen ausreichend Freiräume zu schaffen, die ihn/sie für seine/ihre Expertenstellung in der Organisation benötigt.



5. Evaluation exemplarischer Security Awareness-Materialien

Um Passung bzw. Synergien zu den im Rahmen des Projektes „Awareness Labor KMU (ALARM) Informationssicherheit“ geplanten digitalen und analogen Lernszenarien zu testen, wurden den Teilnehmenden konkrete Beispiele für mögliche Sensibilisierungsmaßnahmen präsentiert.

Es traten jedoch technische Probleme auf, die letztendlich dazu führten, dass zwei der Teilnehmenden nicht hierzu befragt werden konnten. Ein Interview musste aufgrund einer restriktiven Firewall auf einer anderen Plattform geführt werden, auf der sich das Material nicht präsentieren ließ. Ein Tiefeninterview brach kurz vor der Präsentation der einzelnen Formate ab und es ließ sich kein Ersatztermin finden.

Hinsichtlich der Ergebnisse des Materialtests muss ebenso die eingeschränkte Kommunikation infolge der Online-Konferenzen berücksichtigt werden. Vor allem bei den analogen Instrumenten, die auch über ihre haptischen Qualitäten bzw. über die großen Formate (1-2 m große Spielfelder bzw. Wimmelbilder) wirken, muss eine erhebliche Einschränkung bei der Bewertung kalkuliert werden.

Das Testmaterial stammt aus den mehr als einhundert Kampagnen, die die Security Awareness-Agentur known_sense in den letzten 20 Jahren vornehmlich bei Groß- bzw. Konzernkunden in etwa 50 Ländern eingesetzt hat.

Sämtliche Formate werden als Möglichkeiten der mit Security Awareness verbundenen Optionsvielfalt hinsichtlich Format, Kanal, Ansprache, Wirkungsgrad u. v. m. vorgestellt. Dennoch gelingt eine Trennung von Form und Inhalt nur bedingt: Mitunter werden Formate abgelehnt, da das kommunizierte Sicherheitsthema als irrelevant wahrgenommen wird, obwohl die Darbietung an sich als durchaus wirksam erlebt wird. Andere Formate werden gelobt, da das Thema als bedeutsam betrachtet wird – auf Nachfrage stellt sich aber die Form selbst als ungeeignet für das eigene Unternehmen heraus.

5.1 Exkurs: Gamification

- **Definition:** Gamification meint die Anwendung von Spieledesignprinzipien, -designdenken und -mechaniken auf (ursprünglich) spielfremde Anwendungen und Prozesse. Damit will sie Probleme lösen und die Teilnehmenden mit dem Ziel einer Motivationssteigerung interagieren lassen [18]. Beim Einsatz im Kontext Security Awareness unterstützt Gamification, erwünschte Verhaltensweisen zu kommunizieren und über Simulationen einüben zu lassen [19].

Der Begriff „Gamification“ ist weitgehend unbekannt und muss zunächst erläutert werden. Das Prinzip wird von den meisten Befragten als sinnvoll angesehen:

> *„Statt Belehren eher Auflockern. Das ist mal eine lohnenswerte Überlegung.“*
>
> *„Alles besser als Power-Point-Schlachten.“*
>
> *„Was lustig ist, das merkt man sich besser. Das weckt die Vorstellungskraft, bringt Abwechslung und fördert gleichzeitig die Teamfähigkeit – toll.“*

Zugleich darf das Spielerische bei Security Awareness in KMU nicht zu stark in den Vordergrund treten. Dies führt zu deutlichen Widerständen:

> *„Ich darf meinen Leuten aber jetzt nicht sagen: ‚Komm, wir machen ein Spielchen‘. Dann denken die, ich habe was genommen.“*
>
> *„Eher Junge finden das toll, der Rest – auch die Führungskräfte – findet es doof.“*

Diese Haltung zum Spielerischen zeigt sich auch in der Bewertung der präsentierten Materialien. Diese wurden sehr unterschiedlich beurteilt, ein Ranking mit klaren Präferenzen war daher nicht möglich. Über alle Vorlieben für oder gegen bestimmte Formate zeigen sich zwei wesentliche Kriterien, die bei der Bewertung zugrunde gelegt wurden:

- Wird ein Thema seriös oder spielerisch präsentiert?
- Werden klare Regeln und Handlungsanweisungen präsentiert, die ohne große Diskussion akzeptiert werden müssen? Oder verweist das jeweilige Format auf komplexe Zusammenhänge und fordert dadurch zu einer eingehenden kritischen Auseinandersetzung auf?

Nachfolgend werden die Formate kurz vorgestellt und anschließend in eine psychologische Grundmatrix einsortiert.

5.2 Infografik bzw. Lernkarte zum Thema „Social Media – Fake-Profile“

Das DIN A1-Plakat präsentiert typische Hinweise auf Fälschungen in Social Media-Profilen und soll Mitarbeiter/innen sensibilisieren, nicht auf Lockangebote von Cyberkriminellen in sozialen Netzwerken einzugehen. Es wur-

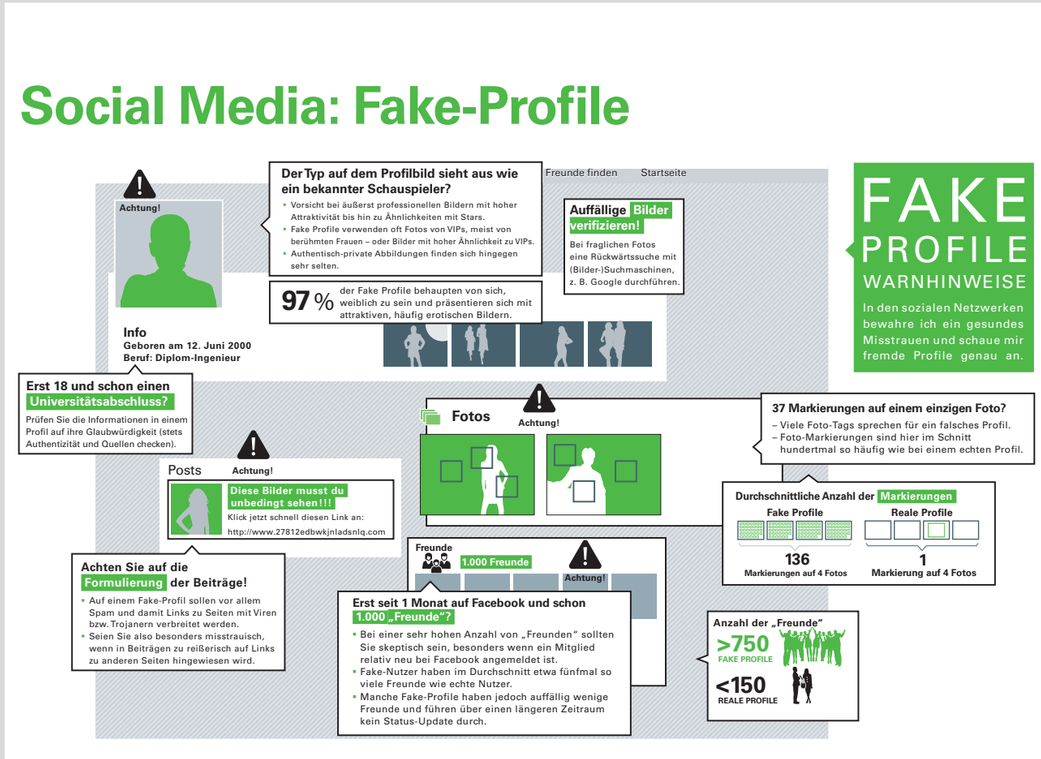


Abb. 4: *Infografik „Social Media – Fake Profile" (Quelle known_sense)*

de bisher von zahlreichen Konzernkunden digital innerhalb des Intranets und als Print (u. a. bei Security Events bzw. Awareness Trainings) genutzt und im Rahmen diskursiver Settings innerhalb didaktischer Formate als Kommunikationsbeschleuniger (z. B. um Diskussionen anzuregen) eingesetzt.

Die Form der Infografik kann nur schwer vom Inhalt getrennt werden. Da die Gefahr von Fake-Profilen von den meisten Teilnehmenden erstaunlicherweise als irrelevant abgetan wird, wird das Format nur von wenigen als sinnvolle Unterstützung bewertet:

> *„Bei uns kein Thema. Wir haben eigene Instagram- und Facebook-Accounts. Da wird aber nur Eigenes hochgeladen."*
>
> *„Das spielt bei Schulen eine Rolle."*

Die Ablehnung betrifft vor allem das offenbar unterschätzte Risiko, denn der visuelle Stil wird grundsätzlich positiv bewertet. Die Reaktanz in Bezug auf das Thema ist vermutlich auf die Abspaltung von Kehrseiten der eigentlich positiv bewerteten Funktionen sozialer Netzwerke zurückzuführen. Das Risiko dort leicht getäuscht zu werden, ist den meisten (nach Stützung) bewusst, zerstört aber das heile Wunschbild eines sozial tadellos funktionierenden Miteinanders auf den digitalen Kanälen.

Zugleich hat das Format „Lernkarte", wie der Titel bereits vorgibt, etwas „lernmäßiges" und wird daher schnell mit „Schule" assoziiert. Auch die Forderungen: „Das ist überladen und macht müde" oder „Es müsste kompakter und einfacher sein" zeigen, dass derartige, eher komplexe Lernkarten im Vergleich zu einfachen Promotion-Postern aufgrund der Rezeptionskomplexität deutlich schlechter bewertet werden. Im Gegensatz zur Rezeption von z. B. Promotion-Poster-Inhalten wird hierbei der notwendige persönliche und psychologische Aufwand vor Augen geführt, der mit Sicherheit generell und hier mit dem Schutz der eigenen Person in sozialen Netzwerken verbunden ist. Das gefällt nicht allen.

Bei vergleichbaren Analysen oder Kampagnen-Umfragen in Konzernen oder anderen Großunternehmen loben die Mitarbeiter/innen überwiegend die Leistung von Infografiken oder Lernkarten als textreduzierte Erklärbilder, bei denen man als betrachtende Person stets etwas Neues entdecken kann, was zu einer wertvollen diskursiven Leistung (z. B. bei Security-Besprechungen innerhalb von Teams oder etwa bei Security Events) führt. Auch das Thema genießt in Großunternehmen einen deutlich höheren Stellenwert, nicht zuletzt weil dort zunehmend Fälle offenkundig werden, in denen Fake-Profile von Cyberkriminellen eingesetzt wurden, um hierüber komplexe Angriffe (CEO-Fraud, APT – Advanced Persistent Thread etc.) zu starten. Bei selektiven Stützungen wird das hiermit verbundene Risiko einzelnen Teilnehmenden aus dem KMU durchaus auch gewahr.

5.3 Comic zum Thema „Passwort"

Der Vier-Bild-Comic (hier ohne Abbildung) aus einer internationalen Kunden-Kampagne zeigt einen witzigen Dialog zweier Protagonisten einer umfangreichen Comic-Reihe. Die Hauptfigur überwindet ihre Schwäche zum Memorieren von „starken" Passwörtern dadurch, dass sie Textfragmente aus bestehenden Tattoos (z. B. Liebeserklärungen an Partner/innen oder die eigene „Mutti") nutzt.

Der Comic spaltet. Die einen finden sich im Thema sofort wieder:

> *„Ja, ich gehöre auch zu denen, die nur ein Passwort haben."*
>
> *„Ich traue auch den Kollegen zu, dass die nur ein Passwort haben."*
>
> *„Das ist ja das, was wir eben besprochen haben: das Passwort unter der Schreibtischunterlage oder am Monitor."*
>
> *„Ich habe zwei Passwörter, die sind so extravagant, dass ich die nicht behalten kann."*

Sie schätzen auch den Stil:

> *„Wenn man das sieht, erwartet man Spaß. Das Tattoo ist lustig."*
>
> *„Warum nicht? Das ist mal was anderes."*
>
> *„Ich mag Comics. Also kann ich mir das auch vorstellen."*

Viele hingegen zeigen sich irritiert.

> *„Wir sind seriös, das Thema ist seriös. Da kann man nicht mit einem Comic kommen, das passt doch nicht."*
>
> *„Bei uns ist zwar der Systemadministrator nicht in der Rolle der Geschäftsführung, er kann aber fast alles überschreiben und ändert auch dauernd Passwörter."*
>
> *„Das würde ich höchstens lesen, wenn ich allein bin."*
>
> *„So etwas sollten unsere Kunden nicht sehen, weil die das unseriös finden könnten. Aber im Internet fände ich das absolut spaßig."*

***Abb. 5** (oben): Wimmelbild „Fallstricke am Arbeitsplatz“*
(Quelle known_sense aus der gleichnamigen Security Arena-Station)
***Abb. 6** (unten): Spielfeld (mit Lösung) der Security Arena-Station „Online-Services, Apps & Co.“ (Quellen: known_sense)*

„Das ist Kinderkacke. […] Das Thema ist zu ernst für diesen Stil. Das ist verletzend“.

Die Erfahrung, dass sich offenbar ein harter Riss in Bezug auf Zustimmung oder Ablehnung bei Comics im Kontext mit Security Awareness auftut, existiert seit dem Launch des vermutlich ersten Corporate Awareness-Comics im deutschsprachigen Raum, „Walt & Friends“, vor mehr als 20 Jahren bei RWE [20]. Die Hälfte aller in Kampagnen-Messungen involvierten Teilnehmenden lässt sich über Comics produktiv in Awareness einbinden, die andere Hälfte lehnt dieses Format vehement ab. Eine ähnliche Haltung existiert auch in Bezug auf das Thema „Gamification“, die sich dennoch grundsätzlich in zwei Punkten unterscheidet. Die Zustimmung gegenüber Simulationen, Edutainment Games oder Lernstationen ist in den letzten 5 Jahren um mehr als 50% gestiegen und lediglich 20% aller Befragten (im Rahmen interner Awareness-Messungen bei Kunden von known_sense) lehnen Spiele verknüpft mit Security Awareness ab.

5.4 Wimmelbild: „Fallstricke am Arbeitsplatz“

Das im Original ca. 170 x 120 cm große Wimmelbild stellt das Spielfeld einer Themenstation aus dem Lernstationsformat „Security Arena“ dar und zeigt 14 Risikoszenarien eines typischen Büroarbeitsplatzes. Es erwies sich bisher als ein sehr beliebtes Format. Das Wimmelbild verdeutlicht: Sicherheit ist komplex. Das ist einigen Interviewten zu viel, wobei die vermeintliche Überforderung auch infolge der Einschränkung von Rezeption der Testmaterialien via Monitor gedeutet werden kann. Gerade bei Führungskräften mit einem Anspruch, als Vorbild aufzutreten, kommt es zu Abwehr:

„Das ist mir zu durcheinander. Das würde ich mir nie ansehen. Das verstehe ich auch nicht.“

„Das ist thematisch sinnvoll, aber reizüberflutend.“

„Können Sie das mal größer stellen? Also ja, da ist viel drin. Aber ich verstehe einiges nicht.“

„Das sind relevante Themen, aber ich hätte die lieber auf mehren Folien und größer.“

Für andere spiegelt sich in der Komplexität der Darstellung die des Themas und der Bezug zur eigenen Arbeitswelt wider. Das Bild ist indes nicht selbstverständlich, sondern verlangt nach Kommentaren, Erklärungen oder Austausch. Die Teilnehmenden erkennen den inhaltlichen Anspruch und Parallelen zu ihrem Arbeitsalltag:

„Da fühle ich mich nicht so wie ein Kleinkind beim Thema Informationssicherheit behandelt.“

„Ordentliche Leute, Männer und Frauen.“

„Da sind einige Stolperstellen dabei, die ich bei den Kolleginnen und Kollegen auch kenne.“

5.5 Security-Arena-Spielfeld „Apps, Online-Services & Co.“

Das im Original ca. 100 x 100 cm große Spielfeld zeigt als Tabelle in der Horizontalen neun populäre Kategorien von Apps mit bekannten Beispielmarken (z. B. WhatsApp). In der Vertikalen sind neun mögliche, mit den Apps verbundene Sicherheits- bzw. Datenschutzrisiken aufgelistet (z. B. Geolocation). In diesem Lernszenario sollen rote Jetons dort zugeordnet werden, wo – bezogen auf die jeweiligen Apps – Risiken vermutet werden, sodass im Gesamtbild auf spielerische Art eine Risiko-Matrix entsteht.

Ohne Erklärungen sind weder Abbildung noch Tool zu verstehen. Das Thema selbst ist für die meisten interessant, aber der Zugang eröffnet sich nicht von allein. Manche sind nicht an dem Spiel interessiert, sondern wollen sich lieber das Bild als präsente Übersicht (nach Art eines „Mahnmals“) an die Wand hängen oder mit dem eigenen Smartphone fotografieren, um jederzeit darauf zugreifen zu können. Andere sehen sich dieses Tool schon in einem nächsten Meeting anwenden und zeigen sich positiv angeregt:

„Das ist interessant. Das ist auch hilfreich zur Einschätzung sowohl privat wie bei der Arbeit.“

„Ich kann mit allen Apps was anfangen. Da ist also der Bezug da.“

„In einem Meeting würde das die Interaktivität fördern statt nur Unterweisung.“

„Das kenne ich von der TH, wunderbar zum Sensibilisieren. Ich weiß aber nicht, in welcher Form ich das einbringen könnte. Aber als Hinweis ist das schön eindeutig.“

In einigen Fällen kommt es zu deutlicher Ablehnung, zumeist weil die korrekte Anwendung – teils aber aufgrund der Darstellungsprobleme am PC – nicht sofort offensichtlich wird:

„Das finde ich nicht gut. Das ist zu unübersichtlich und mir erschließt sich der Sinn nicht auf Anhieb.“

***Abb. 7** (oben): Zwei Monatsblätter aus dem Kalender WATCH IT (Quelle: IWC Schaffhausen, known_sense)*
***Abb. 8** (unten): Artikel Cyber -Grooming aus dem Magazin WATCH IT (Quelle: IWC Schaffhausen)*

„Wie soll das gehen? Verstehe ich nicht."

„Die Tabelle ist viel zu viel zu lesen. Das ist zu theoretisch für ein Spiel."

In vergleichbaren Untersuchungen bei Großunternehmen, die z. B. diese oder ähnliche Lernstationen (z. B. auch „Fallstricke am Arbeitsplatz" mit dem unter 5.4 evaluierten Wimmelbild) einsetzen, fielen die Bewertungen deutlich positiver aus.

5.6 Awareness-Monatskalender-Visuals

Die Visuals eines Awareness-Monatskalenders stammen aus einer umfangreichen Kampagne („WATCH IT") für IWC Schaffhausen (hier u. a. das Beispiel „Homeoffice") und zeigen im Stil von Pop-Art u. a. eine Frau an einem unaufgeräumten Schreibtisch mit einer annotierten Textbox, die Tipps und Tricks zum Thema anbietet.

Mit Erleichterung wird dieses Format sofort verstanden. Dadurch entsteht Raum für eine genaue Betrachtung und Kritik:

„Die Frau versinkt im Chaos. Da bekommt man ja Ärger mit der Gleichstellungsbeauftragten."

„Ich mag den Stil, das fällt auf. Und Homeoffice ist ja auch ein Thema, wobei das bei manchen auch im Büro so aussieht."

Im Gegensatz zu den komplexen (Serious) Games oder dem pointierten Comic verspricht der Kalender eine ruhige und intensive Auseinandersetzung und wurde von vielen als allgemeines Konzept positiv aufgenommen. Manch einer sucht schon den richtigen Platz für den Kalender:

„Ich setze darauf, dass wenn man einen Monat auf ein Bild guckt, dass sich das dann verinnerlicht. In einem Jahr hätte man 12 Themen präsentiert."

„Finde ich gut. Kurz und knapp die wichtigsten Regeln. Und in einem Jahr hätten wir die wichtigsten Themen durch. Also mir gefällt das."

„Das sieht gut aus. Und jede Woche eine neue Regel finde ich gut, z. B. an der Kaffeemaschine."

5.7 Corporate Media-Artikel „Cyber-Grooming"

Hier wurde eine Doppelseite (deutsch/englisch) aus dem Mitarbeitermagazin „WATCH IT" der gleichnamigen Kampagne des Uhrenherstellers IWC Schaffhausen [21] mit einem Artikel über Cyber-Grooming (Anbahnung sexueller Kontakte im Internet) präsentiert.

Private Sicherheitsthemen wie „Cyber-Grooming" gehören als Schlüssel zur bzw. Treiber von Aufmerksamkeit in jede Security Awareness-Kampagne.

Das Thema spricht vor allem die Eltern und im Besonderen Mütter unter den Befragten an, die sehr aufgeschreckt reagieren. Bei zahlreichen Teilnehmenden macht sich jedoch Reaktanz sowohl gegen das Thema, vor allem aber gegen die vermutete „Hochglanz-Umsetzung" breit (Anmerkung: das Magazin erscheint allerdings ausschließlich elektronisch), zumal im eigenen Unternehmen kein Mitarbeitermagazin oder vergleichbarer Kanal existiert.

Bis auf wenige Ausnahmen wird dieses Format auf einem der hinteren oder sogar dem letztem Rang positioniert.

„Das ist ein großes Thema, aber die Eltern wissen das schon selber."

„Das wird doch keiner lesen, das ist zu viel."

„Das sprengt den Rahmen."

„Wir haben kein Mitarbeitermagazin."

Im Gegensatz zu der hier erlebten Reaktanz der KMU werden identische oder ähnliche Artikel bei vergleichbaren Untersuchungen in Konzernen oder anderen Großunternehmen überwiegend sehr positiv bewertet – auch erfahren gut gestaltete Mitarbeitermagazine hohe Reputation von außen: Die Kampagne „WATCH IT" mit dem hier evaluierten Mitarbeitermagazin als Schlüsselmedium erhielt 2020/21 sowohl die Goldene Feder in der Schweiz in der Kategorie „Campaigning" [22] als auch den Award „Care4Aware" in der Kategorie „Branding".

5.8 Poster „Social Engineering"

Den Teilnehmenden wurden zwei von 50 Posterpaaren mit Goldenen Regeln aus der Kampagne „Card of the Month" von T-Systems International (hier zum Thema „Social Engineering") zur Evaluierung vorgelegt.

Eines der Bildmotive zeigt innerhalb einer Kipplogik einen weißen „Wolf im Schafspelz" inmitten einer Schafherde, ein anderes einen Teufel. Intention hinter den Postern ist eine Marketing-Aktion zur Bewerbung von Moderationskarten für Führungskräfte, die monatlich eines von etwa 50 Informationssicherheitsthemen aus der Moderationsbox der Deutschen Telekom innerhalb von Team-Meetings besprechen sollen.

Thema und Bildsprache der Poster sind involvierend gestaltet, sodass kaum über das Format gesprochen wird. Dies zeigt, dass selbst klassische Promotionsformate wie ein Poster durchaus Potenzial für eine packende Dis-

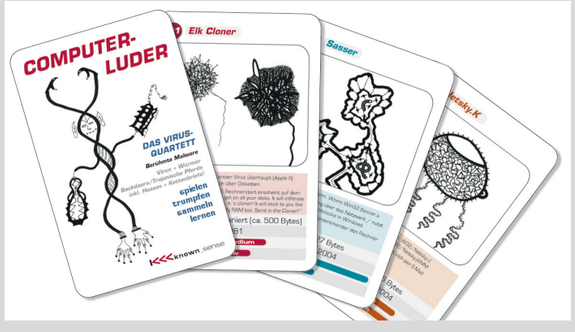


Abb. 9 *(oben): Social Engineering-Poster (Quelle: T-Systems International)*
Abb. 10 *(mitte): Riesenspiel „Quer durch die Sicherheit“ (Quelle: EnBW)*
Abb. 11 *(rechts): Virusquartett „Computerluder“ (Quelle: known_sense)*

kussion haben und es ihnen gelingt, für relevante Informationssicherheitsthemen zu sensibilisieren. Folgende kritische Kommentare wurden zur inhaltlichen Gestaltung der Poster gemacht:

> *„Ein Wolf und ein Teufel – das beeindruckt mich nicht. Und dem Begriff ‚Social Engineering‘ bin ich noch nie begegnet. Das ist kein Thema, auch nicht unter einem anderen Begriff.“*
>
> *„Ganz schlecht, wir sind keine dummen Schafe!“*
>
> *„Es hat einfach zu viel Text. Also ist es nun ein Poster oder bekomme ich das in die Hand?“*
>
> *„Da muss man dann stehen bleiben und lesen. Aber warum muss das auf Englisch sein?“*

Dieselben Motive wurde bereits 2015 im Rahmen der tiefenpsychologischen Social Engineering-Studie „Bluff me if u can – gefährliche Freundschaften am Arbeitsplatz“ [23] evaluiert und als „nachhaltige Büroausstattung“ bzw. Werbemittel zur Begleitung teambasierter Sensibilisierungs-Tools mit didaktischer Intention verstanden.

Exkurs Social Engineering

Der Begriff „Social Engineering“ ist lediglich den IT-Spezialisten und IT-Spezialistinnen bekannt. Von den anderen wird er zum ersten Mal gehört. Die Zusammenhänge von Social Engineering, die Funktionsweisen und mögliche Abwehrstrategien sind weitgehend unbekannt:

> *„Den Begriff kenne ich nicht, aber ich kenne ‚Fake-Account‘. Ich halte es auch für unwahrscheinlich, dass uns etwas in der Richtung passiert […]. Die meisten Mitarbeiter haben nicht so einen tiefen Einblick und wir sind kein produzierendes Gewerbe. Das ist uninteressant.“*
>
> *„Das ist so ätzend wie ‚Industrie 4.0‘: zu abstrakt und niemand über 50 kennt den.“*
>
> *„Dafür sind wir zu klein. Ich denke nicht, dass das bei uns eine Rolle spielt.“*

5.9 Begehbares Riesenspiel „Quer durch die Sicherheit“

Hierbei handelt es sich um ein etwa 25 Quadratmeter großes, aus bedruckten Laminatfliesen bestehendes, kombiniertes Quiz- und Ziehspiel, bei dem Fragen zum Thema „Informationssicherheit“ beantworten werden sollen, um das Ziel auf dem begehbaren Spielfeld zu erreichen (in der Abbildung in einer Version der EnBW) [24]. Statt mit Großfiguren zu spielen, können die Spielenden selbst das Spielfeld betreten und als Spielfiguren agieren. Größe und Aufmachung sollen für Aufmerksamkeit auf Security Events und während moderierter Awareness Workshops sorgen. Das Spiel ist über die begehbare Großvariante auch im kleineren Tischformat mit Spielfiguren im Einsatz. Ähnlich wie bei den o. g. Lernstationen wird eine zusätzliche Sensibilisierungsleistung über eine produktive Moderation (via Train-the-trainer-Konzept) gestützt.

Der spielerische Ansatz muss nicht erklärt werden, sondern steht prägnant im Fokus. Der Event-Charakter und vor allem die Größe des begehbaren Spiels rücken das Thema „Informationssicherheit“ eindrucksvoll in den Blick. Die wenigsten können sich das Spiel im eigenen Unternehmen vorstellen, da dieses Format vor allem durch seine Größe zu aufwendig erscheint und eher als Team Building-Maßnahme verstanden wird – bevorzugt in Großkonzernen. Außerdem werden Bedenken gewahr, dass die eigene Kontrolle an andere Mitspielende abgegeben und man als Spielfigur fremdbestimmt bewegt wird:

> *„Ganz ehrlich, das ist viel zu kompliziert. Da muss ich so viel erklären – nimmt zu viel Zeit in Anspruch.“*
>
> *„Das ist Kinderkacke. Dafür sind wir zu weit. Diesen Level haben wir schon.“*
>
> *„Für die Azubis vielleicht, eher wie Mensch-ärgere-dich-nicht als wie Schach.“*
>
> *„Da würde ich wie eine Schachfigur hin- und hergeschoben werden. Ich würde da auf gar keinen Fall hingehen, wenn ich nicht gezwungen werden würde.“*

5.10 Virusquartett „Computerluder“

Die 32 Spielkarten mit der Hall-of-Fame der Malware und entsprechenden Leistungsdaten bzw. Bewertungen (z. B. Risiken) sind als Trumpfspiel angelegt. Das Kartenspiel, vermutlich das erste Security Awareness Game weltweit, wurde erstmals 2004 von known_sense veröffentlicht und häufig als Awareness Giveaway von Kunden lizenziert. Auf den Kartenrückseiten sind Awareness-Botschaften zum Thema „Malware“ möglich.

Das Prinzip des Quartetts erschließt sich sofort, was positiv bezüglich der Einsetzbarkeit aber auch negativ gegenüber dem Schwierigkeitsniveau gedeutet wird. Es eröffnet also u. a. Erinnerungen – positive wie negative – an vergangene Kinderzeiten.

Abb. 12 *(oben): „Passworthalter" mit Passworthalterkarte (Quelle: EnBW, known_sense)*
Abb. 13 *(mitte links): Screenshot digitales Minigame „Schreibtischtäter" (Quelle: T-Systems International, known_sense)*
Abb. 14 *(rechts): Kartenauszug aus „Talking Security - sprechen wir mal über Sicherheit" (Quelle: known_sense)*

„Das finde ich gut, ist praktikabel. Ich spiele gern Quartett, und das kann man ja jederzeit machen."

„Entschuldigung, das ist jetzt Kindergarten."

„Das wäre ja ein schönes Geschenk für Nerds."

5.11 Security-Moderationskarten „Talking Security – sprechen wir mal über Sicherheit"

Die Moderationskarten mit bis zu 100 (teils projektiven) Fragen zum Thema „Informationssicherheit" (z. B. „Welche Farbe hat Sicherheit?") stellen Gesprächskarten zur kommunikativen Überbrückung schwieriger Situationen von Sicherheitsexperten dar und gelten daher als typische Kommunikationsbeschleuniger für z. B. Team Meetings, Awareness Trainings oder Events.

Das Tool wird unterschiedlich aufgenommen. Es wird sofort verstanden, dass es sich um eine Anleitung handelt, was den Mitarbeitenden mit durchschnittlicher Verantwortung (z. B. Assistierende) daher kaum betrifft. Diese können sich dennoch eine qualifizierte, auf Kommunikation basierte Sensibilisierung als sinnvoll vorstellen. Auch eine Führungskraft freut sich über eine derartige Unterstützung:

„Das ist super cool. Das würde mir helfen, bestimmte Dinge rüberzubringen und greifbarer zu machen. Das wäre ein guter Einstieg in Gespräche."

„Das hätte man dann vor der Pandemie für unsere Meetings nutzen können. Das gefällt mir."

„Das würde ich meinen Abteilungsleitern geben, damit die neuen Mitarbeiter damit standardisiert eingewiesen werden."

Andere Teilnehmenden kritisieren die Themenauswahl oder den ungewohnten Angang mittels projektiver Fragen („Was sollen denn hier die Märchen?"). Sie lehnen das Format konsequent ab, ohne sich weiter auf die Karten einzulassen:

„Unter meinem Niveau."

5.12 Awareness Giveaway „Passworthalter"

Es handelt sich bei diesem Werbemittel um eine Klappkarte, eingeklemmt in einen Konzepthalter, in deren Standfuß der Titel „Passworthalter" eingraviert ist. Auf der Karte wird dazu aufgefordert, ein Passwort in ein freies Feld der Karte zu schreiben. Im Inneren der Klappkarte wird jedoch darüber aufgeklärt, dass diese Aufforderung eine paradoxe Intervention sei und die Angabe des Passwortes zu unterlassen ist. Diese paradoxe Intervention zielt auf eine Auseinandersetzung mit der Passwort-Policy ab und soll den Nutzenden überraschen, z. B. als Incentive bei Trainings und als Werbemittel für laufende Kampagnen.

Der Passworthalter sorgt meist für Heiterkeit. Hinter dem Witz ist aber bei entsprechender Selbstreflexion auch das tatsächliche Problem zu erkennen und spätestens an dieser Stelle wird das Problem des sicheren Passworts erneut thematisiert:

„Dann könnten manche sich veräppelt fühlen."

Eine didaktisch wirksame Sensibilisierung wird durch dieses Awareness Giveaway nicht erwartet. Aber durch die strategische Einbindung in ein Gesamtkonzept könnte es einen wichtigen Sensibilisierungsbaustein darstellen.

5.13 Digitales Clean Desk Game „Schreibtischtäter"

Ähnlich der analogen Lernstation „Clean Desk" aus der Security Arena sollen in dieser zweiminütigen Digitalsimulation 25 Dokumente bzw. Objekte, die typischerweise auf einem Schreibtisch stehen könnten, gemäß der Clean Desk Policy in verschließbare Schubladen gezogen oder stehen gelassen werden [24]. Kunden setzen dieses Minigame als Einzelmaßnahme oder integriert in Web Based Trainings ein.

Das Digitalspiel wird von allen mit Freude und/oder Ehrgeiz durchgeführt. Das Spiel selbst erscheint einigen als „oldschool", andere schätzen den sehr schlichten Charakter. Dennoch ärgern sich alle darüber, nicht die volle Punktzahl erhalten zu haben. Diese Form der Sensibilisierung wird fast durchgehend positiv angenommen, obwohl das Thema „Clean Desk" bzw. „Clear Desk" bei einigen Befragten keine hohe Relevanz hat. Es werden mitunter konkrete Vorschläge für den Zeitpunkt der Einbindung gemacht:

„Das ist nicht schlecht, das merkt man sich."

„Ich finde dieses Spielerische toll. Das bleibt doch viel besser hängen."

„Besser als diese Powerpoints – das kann doch keiner mehr sehen."

„Das finde ich supercool. Für alles bis 40."

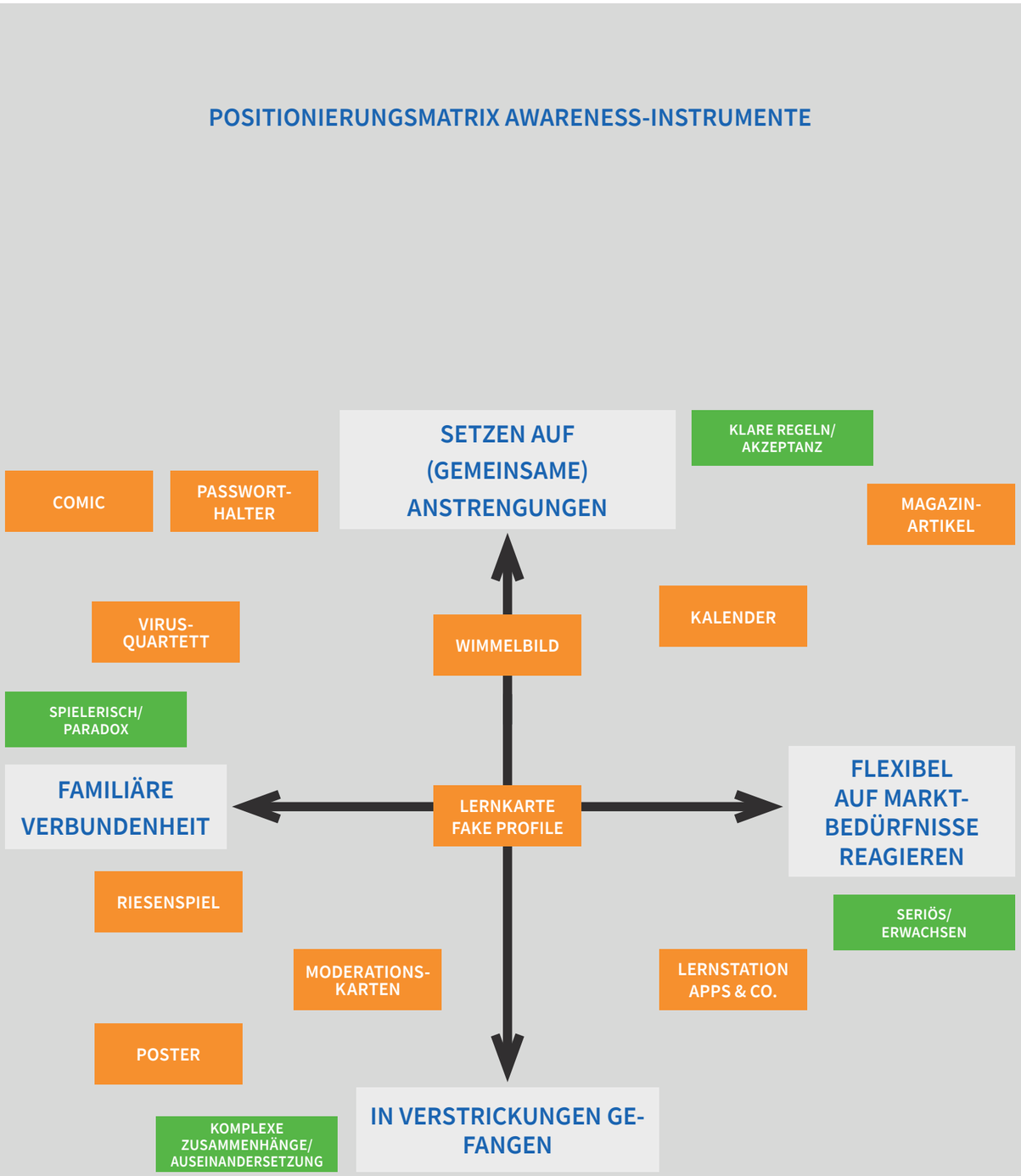


Abb. 15: *Positionierung der Awareness-Instrumente in der psychologischen Matrix von Sicherheitskultur in KMU*

„Ich würde das per Mail vor der Mittagspause schicken. Dann spielt man das und kann sich in der Kantine darüber unterhalten. Das bleibt dann richtig hängen."

„Und wenn man dann noch so auf dem Kalender die Regeln auftauchen, das ist doch dann viel effektiver."

5.14 Zwischenfazit – exploriertes Security Awareness-Material

Formal lassen sich die vorgelegten Security Awareness-Materialien in drei Rezeptionssarten gruppieren:

1. **Grundsätzlich unpassend**, da potenziell zu hohe Kosten oder generell ein zu hoher Stellenwert damit assoziiert werden. Das liegt u. a. daran, dass in der Gesamtwirkung der evaluierten Instrumente eine Konzernkultur dominiert oder der Spielende selbst als Akteur (z. B. bei dem begehbaren Riesenspiel) „zu präsent" sei. Dies betrifft neben Unternehmensspielen mit Statement-Charakter auch „aufwändige Hochglanz-Artikel oder -Videos".

Oder grundsätzlich passend:

2. **Sekundär-Werkzeuge der Security Awareness** („Delegation- oder Promotions-Tools"), z. B. typische Sicherheitsanker bzw. Kampagnenbegleiter wie Kalender, Poster oder andere Key Visuals und Giveaways u. a. typische Below the Line-Tools, deren Rezeption nicht zu zeitintensiv sind und die das Thema über einen längeren Zeitraum mühelos und mehr oder weniger nebenher bewegen.
3. **Change-Tools**, etwa Minigames an Lernstationen und andere Simulationen, Moderationskarten, Selbsttests, diskursives Material, das potenziell simpel zu integrieren ist und „nicht zu sehr nach Großunternehmen aussieht". Diese Formate können spielerisch komplexe Zusammenhänge aufgreifen, zugleich aber klare Handlungsanweisungen bieten und damit Akzeptanz schaffen. Dass hiermit Moderationsleistungen verknüpft sind, die gegebenenfalls interne personelle Ressourcen benötigen, wird mitunter allerdings beiseitegeschoben.

5.15 Psychologische Einordnung Awareness-Material

Die evaluierten Formate lassen sich innerhalb der psychologischen Positionierungsmatrix aus Kapitel 3.6 unterbringen (siehe Abbildung 15 links).

Obwohl das Material-Portfolio nach der pandemiebedingten Absage der Face-to-face-Interviews auf die potenziell schwierigeren Bedingungen der Online-Interviews verändert wurde, erwies es sich als eine große Herausforderung, textlastige bzw. kleinteilige Formate adäquat online zu präsentieren. Teilweise sanken Aufmerksamkeit und Bereitschaft enorm, sich mit Details oder typisch komplexen Zusammenhängen der Informationssicherheit zu beschäftigen. Reaktanz wurde hingegen ausgelöst, sodass mit viel Aufwand motivierend begleitet werden musste.

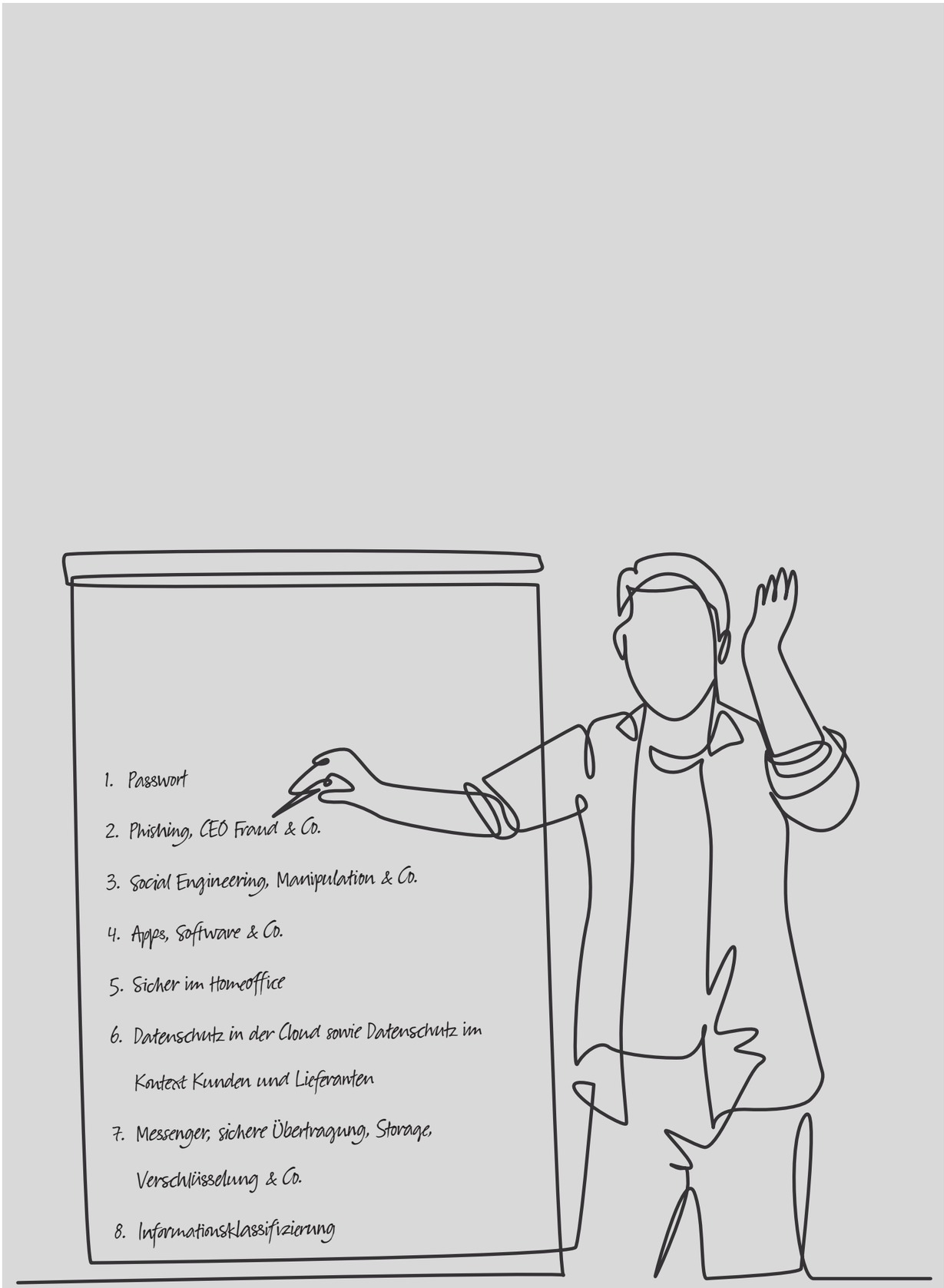
Die Schwierigkeiten beim Durcharbeiten führten oft dazu, dass die Teilnehmenden sich bereits durch das Interview selbst sensibilisiert fühlten und Interesse für mögliche Maßnahmen entwickelten.

Die spielerischen Ansätze werden im ersten spontanen Zugriff von den Mitarbeitern ohne Führungsverantwortung besser platziert als von manchen Führungskräften. Dies könnte ein Hinweis darauf sein, dass Geschäftsführende und Führungskräfte von KMU bisher deutlich weniger mit Unternehmensspielen konfrontiert waren als Mitarbeitende aus Konzernen und noch um eine Positionierung des Themas im eigenen Unternehmen ringen. Mitunter wurden aber noch während des Gesprächs Notizen für mögliche Sensibilisierungsideen gemacht.

Hierdurch und durch die intensive Beschäftigung mit den für viele neuen Optionen wird deutlich, dass spielerische Ansätze den Führungskräften gute Möglichkeiten bieten, das wichtige Thema „Informationssicherheit" neu anzugehen. Dabei tritt jedoch die bislang eher verborgen gehaltene Sorge zu Tage, die Mitarbeitenden tatsächlich zu einem sicheren Verhalten bewegen zu können.

Zugleich wird festgehalten, dass die Formate bestimmte moderierende Fähigkeiten voraussetzen, die aber nicht immer gegeben sind: „Man wird in der Ausbildung nicht sozial trainiert", sagt eine Führungskraft. Daher zweifeln manche der Führungskräfte und Mitarbeitenden, ob bei den eigenen Fachkräften die ausreichenden Fähigkeiten vorhanden sind, eine geeignete Mitarbeiteransprache im Zusammenhang mit Informationssicherheit zu gewährleisten.

Zu den zentralen Aufgaben bei der Heranführung von KMU an den aktuellen Stand von State-of-the-art-Awareness, d. h. dem Stand von Security Awareness anno 2021, gehört die Erweiterung der Perspektive in Bezug auf das, was heute in der internen Kommunikation durch die Spreizung von Formaten, Kanälen und Methoden möglich ist.



6. Relevante Themen für zukünftige Maßnahmen

6.1 Exkurs: „Awareness-Themen“

Sogenannte „Awareness-Themen“ sind im Rahmen von Security Awareness-Maßnahmen vor allem Strukturierungshilfen in der Wissensvermittlung bzw. Awareness-Vermittlung (durch z. B. Lernszenarien oder längere Kampagnen). Ein verbindlicher Themen-Katalog bzw. eine auf empirischen Daten gestützte Klassifikation, wie sie etwa im Bereich des Risikomanagements eingeführt sind, existieren für den Bereich der Sensibilisierung nicht. Aus Sicht der Organisationen macht es Sinn, im Rahmen von Security Marketing von so genannten „Pain Points“ auszugehen, mithin Risiken, die als Problemfelder identifiziert werden und deren Kommunikation an die Mitarbeitenden potenziell zur Resilienz der Organisation beiträgt. Als Beispiel dient hier das Moderationskartenset zur Kampagnenplanung von „askitMeta“ [25]. Aus dieser Perspektive sind Awareness-Themen auch „Priorisierungsanker“. Ihre logische Anordnung im Kontext von z. B. Kampagnennarrativen erleichtert den Einstieg in die Welt der Informationssicherheit.

Verwendete Begriffe von Awareness-Maßnahmen bilden einen Mix aus Angriffsvektoren bzw. Methoden (z. B. Social Engineering, APT), Kommunikationskanälen (z. B. Soziale Netzwerke, Messenger), Methoden bzw. Fachbegriffen der Informationssicherheit (z. B. Authentifizierung) oder bestehen aus eher „weichen“ Sammelbezeichnungen (wie etwa dem mehrdeutigen Begriff „Cyber Security“).

Bei der Entwicklung von Lernszenarien könnten wahlweise Bezeichnung wie „Authentifizierung“ oder „Passwort“ als Themenfelder genutzt oder eine weitere, gegebenenfalls narrative Repräsentanzen gefunden werden. Mit einer Bezeichnung wie „Passwort“ wird ein Themenportfolio vermutlich breiter verstanden und mit weiteren Prozessen wie dem Vergessen verbunden, als es bei seinem wissenschaftlichen Synonym (Authentifizierung) der Fall ist.

6.2 Ungestützte „Awareness-Themen“

Ungestützt werden nur wenige relevante Themen konkret benannt. Alle Befragten nennen Passwörter und Phishing als zentrale Gefahren. Erst durch konkrete Nachfrage bzw. Vorschläge in den Interviews selbst wird den Interviewten deutlich, wie umfassend das Thema „Informationssicherheit“ ist und welche Themenbereiche ebenfalls dazugehören. Das führt zu einem Erkenntnisgewinn, aber auch zu Sorgen und klarer Überforderung einiger Teilnehmenden:

> *„Oh, wenn ich das nun alles höre. Das ist eigentlich echt sehr umfassend. Das vergisst man.“*
>
> *„Hm, das macht mich nachdenklich. Das ist alles Informationssicherheit.“*
>
> *„Stimmt! Vieles weiß man ja, aber das muss man in dem Zusammenhang denken.“*

Abschließend werden ungestützt als relevante Themen deutlich:

- Passwort
- Phishing und verwandte Bereiche
- Datenschutz & Co. (gemeint sind mit dem Hauptthema verwandte Inhalte!)

6.3 Gestützte „Awareness-Themen“

Weitere Themen konnten lediglich gestützt benannt werden. Daraus ergibt sich, gewichtet nach vermeintlicher Präsenz und Wichtigkeit, folgende Reihenfolge:

1. Passwort
2. Phishing, CEO Fraud & Co.
3. Social Engineering, Manipulation & Co.
4. Apps, Software & Co.
5. Sicher im Homeoffice
6. Datenschutz in der Cloud sowie Datenschutz im Kontext Kunden und Lieferanten (kein Mitarbeiter-Datenschutz!)
7. Messenger, sichere Übertragung, Storage, Verschlüsselung & Co.
8. Informationsklassifizierung (nur dort, wo sie als Prozess eingeführt ist)

Aktuell ohne Ranking bleiben die Themenbereiche „Mobile Sicherheit“ bzw. „Sicher unterwegs“. Die niedrige Priorisierung ist auf COVID-19 zurückführen. Ohne Reisebeschränkungen infolge der Pandemie ließe sich hinsichtlich Reisethemen eine höhere Platzierung vermuten.

6.4 Zwischenfazit „Awareness-Themen“

Thematisch ergeben sich aus dem Gesamtportfolio auf den ersten Blick keine relevanten Unterschiede zu den Top-Themen, die in der Regel auch in den Security Awareness-Kampagnen von Großunternehmen behandelt werden. Dort sind jedoch vor allem menschelnde, manipulative Angriffsmethoden wie „Phishing“ oder generell

„Social Engineering“ deutlich an oberster Stelle gelistet. Dies steht im Gegensatz etwa zum Nummer-1-Thema „Passwort“ bei KMU, die Informationssicherheitsrisiken wie Social Engineering für sich selbst offenbar unterschätzen.

Mit dem Verweis auf die bereits in der Einleitung dieses Kapitels beschriebenen, impliziten Bedeutungsebenen kann vermutet werden, dass ein zentraler Themenoberbegriff wie „Passwort“ nicht nur auf Authentifizierung bezogen wird, sondern gegebenenfalls auch Angriffsvektoren oder -methoden umfasst – wie etwa Social Engineering oder Phishing (als Unterbegriff von Social Engineering), mit deren Hilfe Passwörter offengelegt werden können.

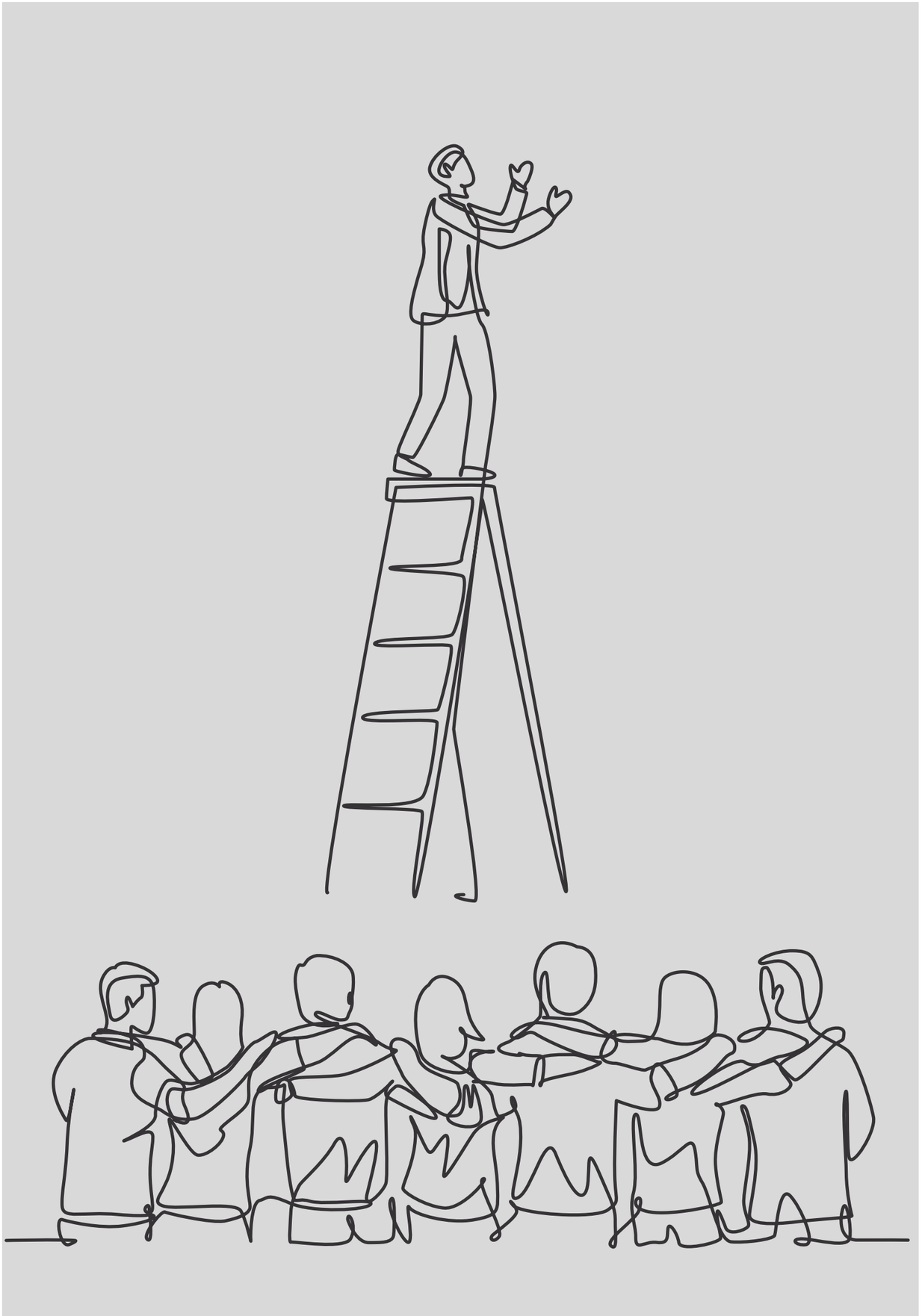
Während dieser Betrachtung der Themenwelten der Informationssicherheit wird deutlich, dass Informationssicherheit als Phänomen stets ganzheitlich zu betrachten ist. Bezeichnungen dienen lediglich als Hüllen für Modelle bzw. Projektionen, die sich oft erst im Kontext von Geschichten bzw. persönlichen Erklärungen eröffnen.

Dies kann als Hinweis dafür gewertet werden, dass es Narrative mit Bezügen aus der Lebens- und Arbeitswelt der Zielgruppen bedarf, um Lernszenarien und andere Sensibilisierungsinstrumente entsprechend nachvollziehbar zu gestalten.

7. Learnings, Fazit und Empfehlungen, Ausblick

7.1 Key Learnings: Die 10 wichtigsten Erkenntnisse dieser Studie im Überblick:

1. **KMU kultivieren Beziehungen und ihren individuellen Produktionsstolz:** Die Probanden/innen sind stolz, Teil einer kleinen, beziehungsstarken Gemeinschaft zu sein, die als Team Außergewöhnliches leistet. Implizite Kehrseiten können jedoch zur Kannibalisierung von Informationssicherheit führen, d. h. einen negativen Effekt auf die Sicherheit ausüben.
2. **Informationssicherheit wird beinahe ausschließlich von außen getrieben:** Informationssicherheit spielt in KMU eine zunehmend wichtige Rolle. Die Entwicklung wird jedoch vor allem von extrinsischen Faktoren bestimmt, bei denen Cyber-Risiken, Regularien und Kunden als Treiber fungieren.
3. **Informationssicherheit erscheint den meisten Mitarbeitenden als Sammelbegriff noch zu diffus und wird von ihnen an die internen Experten oder die externen Dienstleister delegiert:** Die fehlende klare Abgrenzung des Begriffs „Informationssicherheit“ von „Datenschutz“, „Compliance“ und anderen Security-Themen als „eine Sicherheit“ sowie mitunter unklare Zuständigkeiten erschweren häufig die Perspektive auf eine transparente Strategie und fördern abspaltende Tendenzen ohne Wahrnehmung der eigenen Verantwortung.
4. **Eine Security Awareness-Strategie bei KMU ist hinter einer gut gemeinten Intention bislang nicht erkennbar:** Awareness wird aktuell noch relativ limitiert als Synonym für wenig gerahmte Direktdialoge oder eher intuitiv generierte, rein kognitive, lerntheoretische Aktivitäten betrachtet, bei der Sicherheits-Know-how wie einst das Schulfernsehen in die Mitarbeitenden „implementiert“ werden soll (s. Ebene 1 auf S. 15).
5. **Der Nachhaltigkeit sichernde Aspekt „Talking Security“ ist in Ansätzen vorhanden:** Die im Vergleich mit Großunternehmen herausragende Ausgangsposition überschaubarer Unternehmensgröße mit der Option diskursiver Awareness (z. B. Face-to-face) wird zwar in KMU intuitiv genutzt, ist aber strategisch noch nicht ausreichend unterfüttert.
6. **Security Awareness „as a product“ (z. B. als Produkt-Suite) funktioniert nicht:** Generische Awareness-Materialien (z. B. in Form von oft verwechselbarer Web Based Trainings, die als Awareness-Produkt von u. a. IT-System-Anbietern eingekauft werden, bilden nicht die jeweilige Sicherheitskultur ab, sind wenig involvierend und bleiben in der Regel wirkungslos bei relativ hohen Kosten.
7. **Keine Awareness ohne Regeln:** Das Image von Informationssicherheit bzw. Security Awareness leidet auch unter einer Konsequenzlosigkeit bei Verstößen, die für das familiäre Klima in einem KMU typisch zu sein scheint.
8. **Gamification belebt die Phantasie, erfordert aber einen Plan, involvierende Narrative, ansprechende Formulierungen (ein KMU-gerechtes Wording) und den Austausch mit Gleichgesinnten:** Die Einführung von spielerischen und erlebnisorientierten Lernszenarien darf nicht ohne strategische Vorbereitung und regelmäßige inhaltliche Begleitung erfolgen. D. h., spielerische bzw. humorvolle Maßnahmen müssen mit strategischer, respektvoller Ansprache flankiert werden – das Spielerische darf nicht zu sehr in den Vordergrund treten, um die Akzeptanz nicht zu gefährden (z. B. bei Benennung eben „Lernszenario“ statt „Spiel“ – oder „Personalentwicklungs-Simulation“ statt „Gamification“ oder „Planspiel“)
9. **Awareness-Reifegrad spricht gegen eine kurzfristige Diversifikation:** Hinsichtlich Tätigkeits-, Sicherheits- bzw. Kompetenzprofilen konnte infolge von Heterogenität und geringer Awareness-Reife keine psychologische Relevanz ermittelt werden. Der Aspekt der Profile muss in weiteren bzw. nachfolgenden Evaluationen genauer betrachtet werden.
10. **Kontrolle ist gut – (Selbst-)Vertrauen ist besser:** Führungskräfte sind auch nur Menschen und brauchen Bestätigung und Respekt, um ihren Mitarbeitenden selbstbewusst und wertschätzend Vertrauen entgegenbringen zu können. Wenn z. B. eine Führungskraft einen Fehler macht, sollte damit offen umgegangen werden. Dies sollte als ein produktiver Anlass betrachtet werden, zu vermitteln, dass Wissen nicht alles ist und wir alle nur Menschen sind und Fehler machen dürfen. Mitarbeitende brauchen Selbstvertrauen und Vertrauen in ihre Führungskräfte, um sich so sicher wie möglich verhalten zu können. Beide benötigen Rückendeckung und Unterstützung in der Kommunikation. Vor allem Geschäftsführung und IT-Verantwortliche müssen sich intensiver miteinander austauschen.



7.2 Fazit und Empfehlungen

Die hohe Identifikation und Verbundenheit mit zum Teil engen Bindungen und Produktionsstolz in den explorierten KMU schaffen Loyalität und bei der Führung ein hohes Vertrauen in die Mitarbeitenden. Die Kehrseiten des harmonischen Miteinanders einer familiären Kultur wirken sich jedoch zum Teil kontraproduktiv auf die Informationssicherheit aus.

Das Finden von flexiblen Lösungen sowie der vertraute Umgang miteinander vor dem Hintergrund einer überschaubaren Mitarbeiterzahl, die diskursive Wissensvermittlung leichter gestalten lassen als in Konzernen, gehören zu den potenziellen Vorteilen der KMU, führen aber gleichermaßen zu kritischen Entwicklungen. In KMU sind dies teilweise laxe Reglementierungen mit nicht zu striktem Einhalten von Sicherheitsrichtlinien. Die scheinbare Freiheit kann das unternehmerische Handeln fördern, ignoriert aber Risiken und ein intendiertes Gesamtbild „Informationssicherheit“ sowie den Nutzen von Security Awareness. Dabei verkehren sich die Stärken der KMU in ihr Gegenteil: das flexible Reagieren auf externe Anforderungen führt im Bereich der Sicherheit zu kreativ-individuellen Lösungen (z. B. Schatten-IT) und toleriert nicht selten klare Sicherheitsverstöße.

Als bedenklich muss die (Selbst-)Wahrnehmung der Teilnehmenden mit Abspaltung bzw. Abwertungen von real existierenden Angriffsvektoren der Cyberkriminalität, insbesondere die Abwehr von Themen wie „Social Engineering“ oder „Fake-Profile“ im Rahmen der Tests von Sensibilisierungsinstrumenten in Kapitel 5, bewertet werden. Dabei wird aber deutlich, dass Interesse und Beteiligung eine Frage von Ansprache und Terminologie ist. Bei der Präsentation der im Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ zu produzierenden Lernszenarien sollte daher auf die Formulierung geachtet werden (genauer auf die gewählte Terminologie der Instrumente und ihrer Kommunikation), die KMU-kompatibel auszurichten ist.

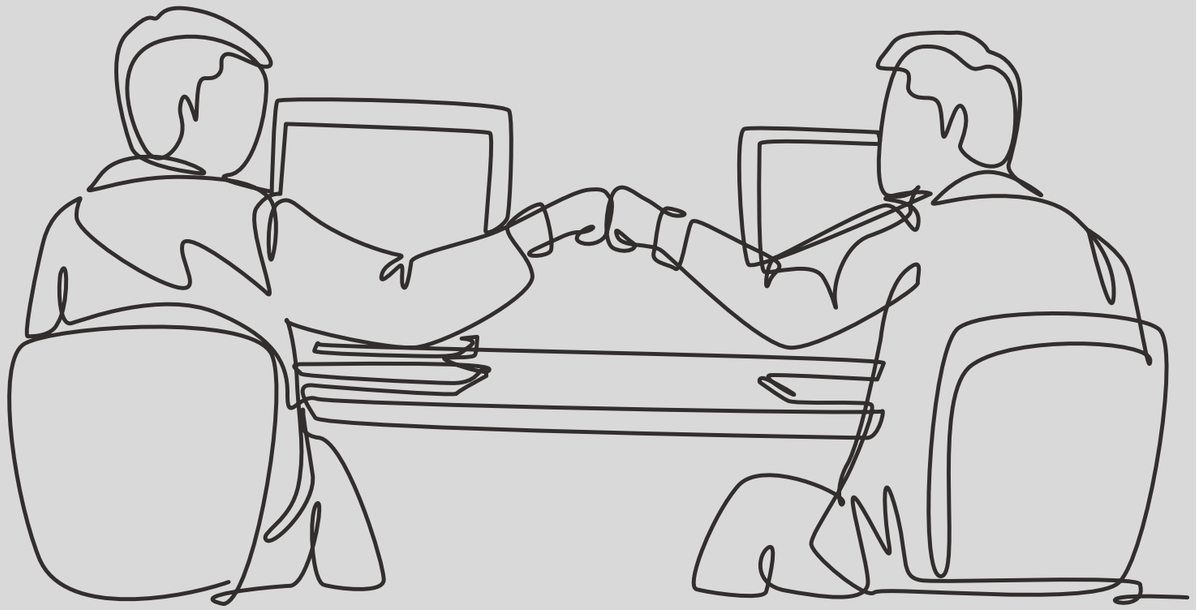
Dabei befinden sich die KMU in Abgrenzung zu Großunternehmen in der eigentlich bequemen Ausgangssituation, dass sie von überschaubarer Größe sind und die einzelnen Mitarbeitenden gezielter und ohne große Streuverluste in Bezug auf Sicherheitsthemen ansprechen können. Dafür benötigen sie noch nicht einmal Marketing-Instrumente (aus dem Ebene 2 des Security Awareness-Framework) als Stellvertreter bzw. Kommunikationssbeschleuniger für die Security-Protagonisten. Gerade das diskursive Prinzip „Talking Security“ (Ebene 3 des Security Awareness Framework) wird intuitiv für persönliche Auseinandersetzungen zum Thema genutzt – häufig allerdings ohne methodischen Hintergrund – und weder dauerhaft, noch strategisch eingesetzt (vgl. auch S. 15-17).

Während also die überschaubare Größe intuitiv eines der Grundprinzipien der Security Awareness, „Talking Security“ aus der Ebene 3, potenziell fördert, verhindern systemische Fallstricke des familiären Miteinanders das klare Ansprechen und das Durchsetzen von Sicherheitsregeln. Gefahren drohen zunehmend durch sorglose Mitarbeitenden und deren Vorgesetzten, die aktuell akute Bedrohungen wie Social Engineering oder ATP abspalten und deren Selbstwahrnehmung mitunter stark von der realen Bedrohungslage abweicht.

Zwar ist den Geschäftsführenden und Mitarbeitenden der befragten KMU die Bedeutung der Informationssicherheit bewusst, wenngleich ungestützt oft nur wenige Themen („Passwort“, „Phishing“, etc.) als Bedrohung erwähnt wurden, die sich von denen der Großunternehmen kaum unterscheiden und in Bezug auf ihre Vertiefung Potenzial für eine hohe Differenzierung bieten. Allerdings werden Risiken auf den ersten Blick hauptsächlich als von außen kommend gesehen, während die gemeinsamen Anstrengungen aller betont und trotz der evaluierten Lücken in der Regel als ausreichend betrachtet werden.

Von außen kommend ist auch der Druck der Kunden zu verstehen, denen man sich als sicherheitsbewusster Dienstleister präsentieren möchte, bei dem die Kundendaten sicher aufgehoben sind. Security Awareness ist als Teildisziplin von Sicherheitskommunikation das „wärmende Lagerfeuer“ der Informationssicherheit. Hier menschelt es deutlich mehr, werden mehr Defizite aufgezeigt als in den rein technischen und prozessualen Security-Disziplinen, so dass Sensibilisierung nicht länger nur als ein Change-Programm begriffen wird, um die Mitarbeitenden beim selbstverantwortungsvollen Schutz der eigenen Organisation zu unterstützen, sondern auch um Kunden, Partner und die Öffentlichkeit zu beeindrucken. Somit etabliert sich Security Awareness zunehmend auch als ein Reputationsinstrument, das den Vertrauensgrad zwischen Dienstleister und Kunde zu beeinflussen vermag. Zahlreiche Großunternehmen haben den Reputationsprozess strategischer Security Awareness etabliert und teilen erfolgreiche Maßnahmen als Good Practice mit Kunden und Partnern. Sie bemühen sich auch um Awareness als Imagefaktor mithilfe von Öffentlichkeitsarbeit, so dass über den erzielten Reputationsgewinn Rückkoppelungseffekte nach innen hinsichtlich des ursprünglich intendierten Mitarbeitenden-Change erzielt werden können.

Auch bei den befragten KMU spielt das Thema „Reputation“ im Kontext von Security Awareness eine (wenn auch untergeordnete) Rolle. Eine strategische Lösung, die im Kontext Security Awareness und Awareness-Messungen verstanden wird, ist allerdings noch nicht sichtbar. Das Thema „Reputation“ schwingt jedoch in den Interviews mit denjenigen Führungskräften unbewusst mit, die ihren persönlich erlebten Druck mit dem Thema



„Informationssicherheit“ vor allem an den Kunden ausrichten. Gerade die mitunter erlebte Abwertung gamifizierter Anteile bei den Führungskräften ist als Projektion zu deuten. Hier wird die vermeintlich abwertende Perspektive der Kunden eingenommen. Nach Vorstellung vieler Führungskräfte würden sämtliche Anstrengungen im Kontext von Informationssicherheit ins Leere laufen.

Eine Akzeptanz – gerade der spielerischen Ansätze – könnte allerdings bereits durch ein kompatibles Wording reguliert werden. Gerade in KMU ließe sich durch die vermeintlich seriösere Bezeichnung „Simulation“ anstelle von „Spiel“ (auch nicht „Planspiel“) die Bereitschaft zur Teilhabe auch bei konservativen Mitarbeitenden oder Führungskräften und gegenüber Kunden erhöhen. Dennoch müssen die dahinterstehenden Prinzipien und der Mehrwert spielerischer Formen von Maßnahmen erläutert werden – ansonsten droht Ablehnung. Hierzu gehört auch eine passende narrative Einbindung. Allein der Hinweis, dass in Unternehmen bereits unbewusst Spielprinzipien wie z. B. Rankings genutzt werden, kann eine ablehnende Haltung in Bezug auf Gamification erden. Auch die Tatsache, dass jegliche menschliche Entwicklung durch spielerische Aspekte angestoßen wird – ja dass die Menschheit überhaupt nur existent ist, weil sie sich infolge von Spielprinzipien weiterentwickelt hat, dürfte massive Reaktanz zumindest aufweichen. Als eine Art Argumentationsfibel „pro Spiel“ sei in diesem Kontext auf das Buch „Rettet das Spiel“ [26] von Gerald Hüther und Christoph Quarch hingewiesen.

Auch wenn verbal der Informationssicherheit eine große Bedeutung zugesprochen wird, zeigt sich bei den Pilotunternehmen, dass eine intakte Sicherheitskultur mit ausreichender Sensibilisierung noch nicht bestehen und aktuelle Entwicklungen in der internen Kommunikation (Formate, Methoden etc.) noch nicht ausreichend berücksichtigt oder wertgeschätzt werden.

Dennoch werden Entwicklung und Bereitstellung von allen Teilnehmenden grundsätzlich positiv angenommen und die spielerischen Ansätze geschätzt.

Dabei wird auf Basis der Evaluation von Themen und Formaten aus den Kapitel 4 und 5 deutlich, dass es bei der Entwicklung von Sensibilisierungsinstrumenten neben der Berücksichtigung von Tätigkeits-, Sicherheits- bzw. Kompetenzprofilen auch die Herleitung psychologischer Verfassungen und Lerntypen und deren Vorlieben für unterschiedliche Formate wichtig sein kann. Denn der Test der Formate hat gezeigt, dass nicht jede Mitarbeiterin oder jeder Mitarbeiter mithilfe von emotionalen Ansätzen wie Serious Games, Comics u. ä. zu involvieren ist. Je mehr Kanäle Organisationen also nutzen, um die wichtigen Security-Kernbotschaften zu transportieren, umso geringer fällt der Streuverlust innerhalb der Kommunikation aus. Potenzielle Redundanzen sind dabei zu vernachlässigen, denn nicht jeder hört mit demselben „Format-Ohr“ bzw. „Kanal-Ohr“ [27].

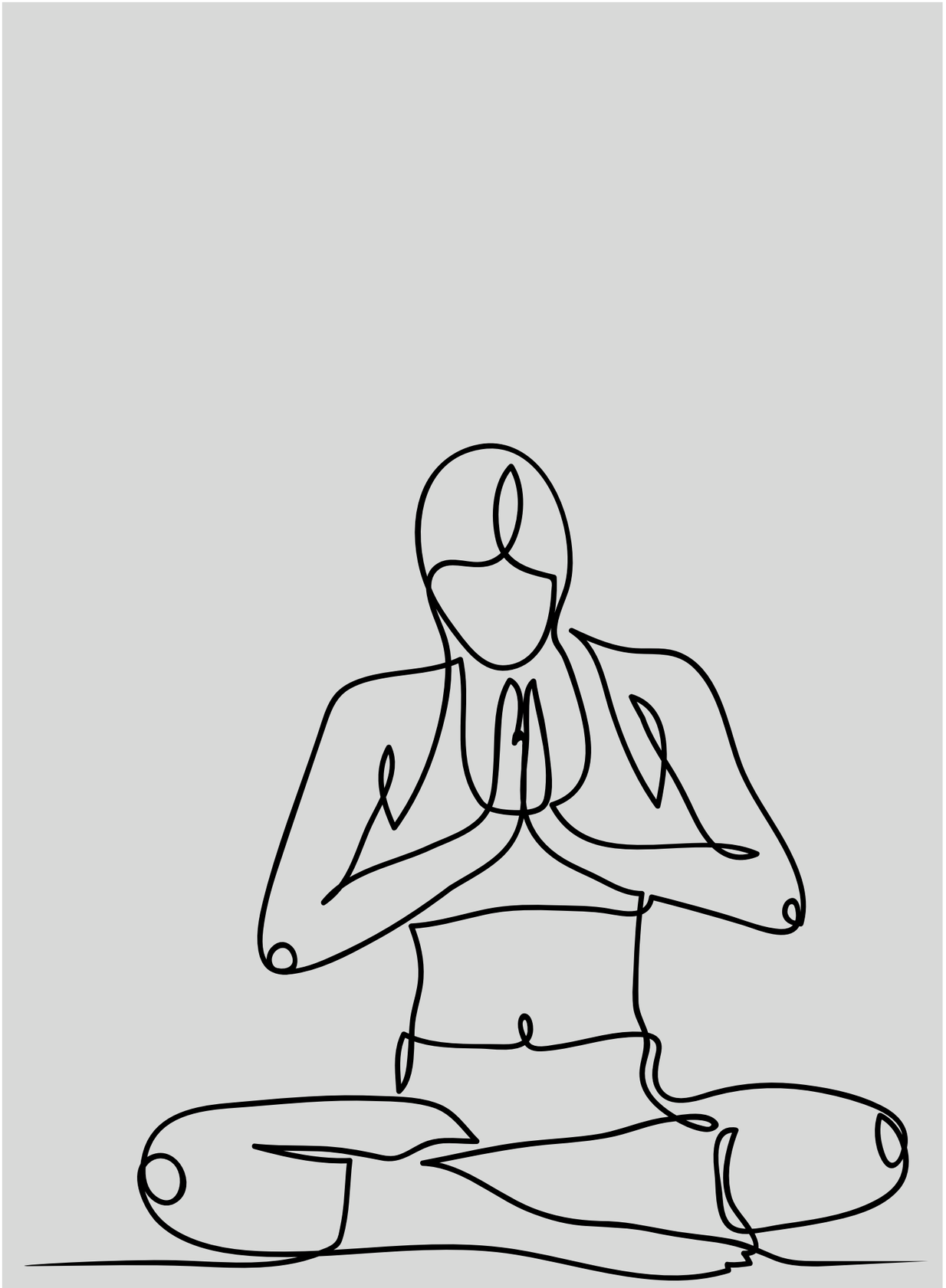
Anders als bei vergleichbaren Analysen oder Umfragen in Großunternehmen erschließen sich allerdings die Intentionen mancher evaluierter Awareness-Formate nicht im ersten Zugriff bzw. ohne erläuternde Kommentare. Der Grund dürfte sein, dass Mitarbeitende von Konzernen regelmäßig und häufiger mit Maßnahmen der internen Kommunikation penetriert werden. Für die Informationssicherheit der Konzerne wird bei der Wahl der Formate und Kanäle in Abstimmung mit den Kommunikationsabteilungen in der Regel auf Bewährtes gesetzt, das deutlich vielfältiger ausfallen dürfte als die Maßnahmen der diesbezüglich limitierten KMU. Dass Corporate Media-Kanäle wie Intranet oder Mitarbeitermagazine in KMU nicht oder zurückhaltend bespielt werden, verfestigt sich. Daher ist die Reaktanz auf Maßnahmen, die als typische Formate der Großkonzerne erkennbar sind, erklärbar.

Eine zielgruppenspezifische Diversifikation von Themen, Vertiefung in Themendetails bzw. Sensibilisierungsmaßnahmen erscheint jedoch nur dann sinnvoll, wenn in den Organisationen bereits ein höherer Awareness-Reifegrad, z. B. infolge einer mehrjährigen, permanenten kommunikativen Penetration, vorliegen würde. Die an dieser Studie beteiligten KMU befinden sich in Bezug auf Security Awareness noch am Anfang eines auf dauerhafte Sensibilisierung ausgelegten Reifegradmodells, das ungeachtet der oben genannten Profile eine Rundum-Versorgung mit Basis-Awareness für sämtliche Zielgruppen und nicht nur für bestimmte Rollen erfordert.

Positiv lässt sich aber aus der Typologie (Kapitel 4) ableiten, dass für beinahe jede der fünf evaluierten Strategien im Umgang mit Informationssicherheit und den damit verknüpften Prototypen ein Zugewinn infolge einer potenziellen Teilnahme an Security Awareness-Maßnahmen abzuleiten ist. Der nachhaltig intendierte Wert der hiermit verknüpften Vorteile steigt mit der zielgenauen Ansprache jedes einzelnen Typus‘.

Am Ende reicht vermutlich die bloße Bereitstellung von Online- oder analogen Awareness-Tools nicht aus. Viele Geschäftsführende und Führungskräfte benötigen Unterstützung bei der konkreten Ansprache ihrer Kunden und Mitarbeitenden, bei der nicht nur die jeweiligen Maßnahmen, sondern auch Idee und Intention dahinter im Kontext mit dem jeweiligen Geschäftsmodell präsentiert werden sollten. Geschäftsführende und Führungskräfte von KMU können sich eben nicht auf eine „Lex-CEO“ berufen und permanent eigene Vorstellungen durchsetzen, vielmehr gilt es die Nähe zum jeweiligen Kunden und Mitarbeitenden zu nutzen und zugleich das gewünschte Sicherheitsverhalten der eigenen Organisation durch konsequentes Feedback zu steuern.

Hierbei ist eine Form von Unterstützung nötig, die begleitend zu den geplanten Lernszenarien implementiert werden sollte. Die Sicherheitstreiber in den KMU müssen



in Bezug auf Sensibilisierung erfahren, dass nachhaltige Awareness vor allem den diskursiven Effekt (Sprechen über Sicherheit) und damit die Auseinandersetzung mit ihren Mitarbeitenden benötigt. Dies umfasst auch die Art und Weise, Mitarbeitende produktiv anzusprechen, wie beispielsweise in Form einer Gebrauchsanleitung für die im Projekt „ALARM Informationssicherheit“ entworfenen Tools.

Ein schriftlicher Leitfaden oder ein Train-the-trainer-Konzept, das die Terminologie des komplexen, interdisziplinären Gesamtthemas sowie die vielfältigen Optionen bzgl. der internen Kommunikation erklärt, jedoch ausschließlich kognitiv-rational ohne sinnliche Erfahrungen vorgeht, wird vermutlich nicht ausreichen. D. h., die Geschäftsführung bzw. das Management brauchen neben diesem Sicherheits-Briefing in Form z. B. eines schriftlichen Awareness-Leitfadens idealerweise auch ein Netzwerk Gleichgesinnter (vergleichbar mit einem Awareness-Kongress – aber ausschließlich für KMU – oder eines Roundtable Awareness KMU mit Good Practice-Sharing nach dem Vorbild des Dax-30-Roundtable Security Awareness) und eine regelmäßige Face-to-face Awareness-Begleitung, bei der auf die dynamische Entwicklung, dem Stand der Awareness und auf potenzielle Barrieren laufend eingegangen werden kann. Die Protagonisten müssen dabei Awareness mit allen Sinnen erfahren, d. h. quasi schmecken und riechen, berühren – dies benötigt personelle Ressourcen und z. B. auch ein Coaching bzw. Supervision, mithin professionelle Kommunikations-Services, die von außen auf das jeweilige System und die hiermit verbundene Kultur schauen.

Die Ausgangslage für einen persönlichen Umgang mit dem Thema ist aufgrund der geringen Größe und damit größeren Reichweite der Geschäftsführenden und IT-Administration im Verhältnis zu den Großunternehmen durchaus vorhanden. Dieser Vorteil kann sich aber, wie beschrieben, in Bezug auf die Kehrseiten in einen Nachteil wandeln.

7. 3 Ausblick

„Security Awareness“ ist als eine junge Disziplin noch nicht einmal drei Jahrzehnte alt. Perspektiven, Methoden, Inhalte und viele andere Bestandteile von Awareness wachsen mit den Risiken der Informationssicherheit und ihren Anforderungen.

So gehört etwa die Integration von z. B. Gamification gar nicht mal zu den neuesten, innovativen Methoden von Sensibilisierung. Ausgehend vom Virusquartett von 2004 werden spielerische Prinzipien seit 17 Jahren versucht zu integrieren.

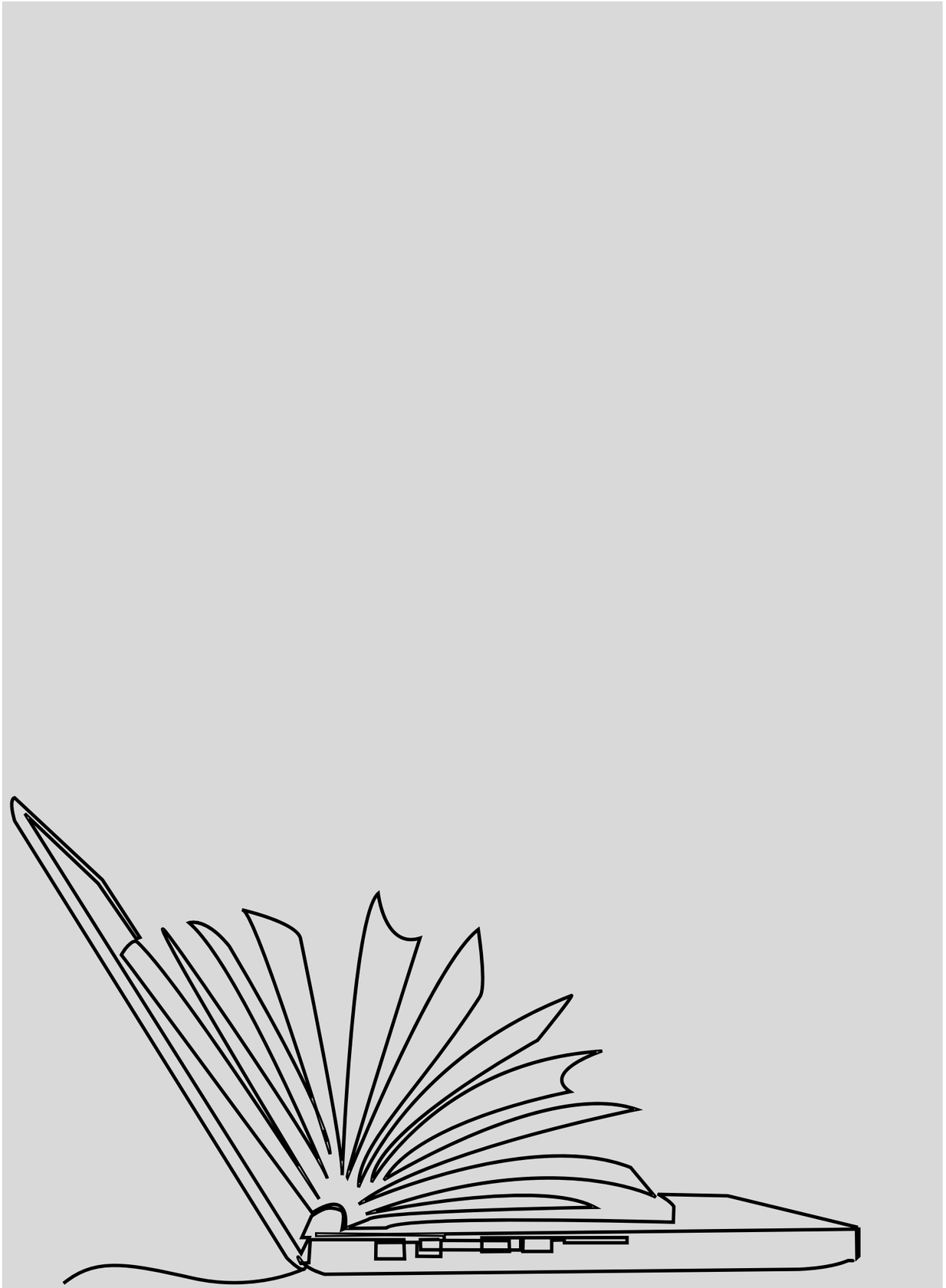
Aktuell bemühen sich etwa zahlreiche Konzerne, die positive Erfahrung mit dem Thema „Achtsamkeit“ in Bezug auf Work-Life-Balance bzw. generell Gesundheitsprävention ihrer Mitarbeitenden machen konnten, darum, die Vorteile von Achtsamkeit (oder MBSR – Mindfulness Based Stress Reduction) in Bezug auf einen gelassenen Umgang mit Risiken zu evaluieren [28]. Das Awareness-Rad mit den vielen Bezügen zu interdisziplinärer Methodik dreht sich also munter weiter.

Die im Projekt „ALARM Informationssicherheit“ zu entwickelnden Handlungsmaßnahmen und konkreten Empfehlungen verkörpern zudem die Botschaft der notwendigen Inhalte und ließen sich in Bezug auf das Akronym z. B. auch folgendermaßen auflösen:

A – Achtsamkeit
L – Lernen & Simulieren
A – Augenhöhe
R – Regelmäßigkeit
M – Miteinander

In diesem Sinne ist es wichtig, dass die KMU nicht versuchen, Großunternehmen zu kopieren, sondern ihren eigenen Weg mit ihren eigenen Bedingungen und Mitteln finden, um die „Human Firewall“ in ihren Organisationen zu aktivieren bzw. weiter zu stärken.

Risikogeriebene ALARMierung ist die eine Seite der Informationssicherheitsmedaille – die andere ist das Aushalten von Fehlern, Kritik und – als eine Stärke von KMU – die Gemeinschaft mit dem KMU-eigenem Produktionsstolz, die es zu sichern gilt, ohne die Kehrseiten zu groß und zu mächtig werden zu lassen.



Literatur

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

[2] Krämer, W., Mittelstandsökonomik. München: Vahlen, 2003

[3] Gesamtverband der Deutschen Versicherungswirtschaft e. V., Cyberrisiken in produzierenden Gewerbe. Berlin, 2021

[4] https://alarm.wildau.biz. Zugriff: 03.05.2021

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

[6] www.known-sense.de/strategie-entwicklung. Zugriff: 03.05.2021

[7] ISO/IEC 27001: 2017. Berlin: Beuth, 2017

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

[9] theospas (Hrsg.), Laudatio zum Outstanding Security Performance Award für das Lebenswerk von Dr. Christoph Schog, T-Systems International, Kent, 2020

[10] Helisch, M., Pokoyski, D., (Hrsg.) Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Springer Vieweg, 2009.

[11] Imdahl, I., Wertvolle Werbung. rheingold-Newsletter, 1. Köln, 2006

[12] https:// www.known-sense.de/Methoden. Zugriff: 15.06.2021

[13] known_sense, Tiefenpsychologische Konzeptanalyse mySecurity & Privacy Box bei T-Systems International, Köln, 2010

[14] https://www.known-sense.de/tiefenpsychologie. Zugriff: 15.06.2021

[15] https://www.rheingold-salon.de/marktforschung-services/. Zugriff 03.05.2021

[16] Schmidt, H., Gondolf, J., Haufs-Brusberg, P., Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU). Hochschule Düsseldorf: Medien, Düsseldorf, 2018

[17] Hillebrand, A., Niederprüm, A., Schäfer, S. Thiele, S., Henseler-Unger, I., WIK Report. Aktuelle Lage der IT-Sicherheit in KMU. Bad Honnef: WIKI Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, 2017

[18] Gabler Wirtschaftslexikon. Wiesbaden: Springer Fachmedien, 2018

[19] Pokoyski, D., Spiel Dich sicher! Security und Gamification. In: <kes> 2018 #2, Frechen: Datakontext, 2018

[20] RWE (Hrsg.) IT-Sicherheit für den RWE-Konzern, Essen: 2007

[21] Helisch, M., Pokoyski, D., Care4Aware. In: TAKE AWARE sec&life magazine 3. https://www.take-aware-events.com/storage/app/media/pdf/takeawaresecandlifemagazine03.pdf. Zugriff: 16.06.2021

[22] https://geschaeftsrisikocybersecurity.de/awareness-kampagne-watchit/ Zugriff: 15.05.2021

[23] 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

[24] https://www.known-sense.de/game-it-securityspiele. Zugriff: 03.05.2021

[25] Beyer, M., Pokoyski, D., askitMeta – Security Awareness-Planungs- und Moderationskarten. Köln: known_sense, 2008

[26] Hüther, G., Quarch, C., Rettet das Spiel, München: Hanser, 2016

[27] Schulz von Thun, F. , Miteinander reden 1. 48. Aufl. Reinbek bei Hamburg: Rowohlt, 2010

[28] Haucke, A. Pokoyski, D., MBSR = Mindfulness Based Secure Reaction? In: TAKE AWARE sec&life magazine 3. https://www.take-aware-events.com/storage/app/media/pdf/takeawaresecandlifemagazine03.pdf. Zugriff: 16.06.2021

Glossar

Abspaltung
Bezeichnet in der Psychologie das Auseinanderfallen von psychischen Funktionen, die im „Normalfall“ als „zusammenhängend“ wahrgenommen werden. Betroffen sein können u. a. neben der Wahrnehmung auch Bewusstsein, Gedächtnis, Identität oder Körperempfindungen.

Advanced Persistent Thread (APT)
Englisch für „fortgeschrittene andauernde Bedrohung“. Ein im Kontext von Cyber-Bedrohung verwendeter Begriff für einen gut vorbereiteten, oft lang anhaltenden, komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen bzw. vertrauliche Daten von Organisationen, basierend auf unterschiedlichen Angriffsvektoren, u. a. auch Social Engineering (s. a. „Social Engineering“ und Kap. 6.1 dieser Studie).

askitMeta
Von der Awareness-Agentur known_sense zusammen mit dem Awareness-Experten Marcus Beyer entwickeltes Moderationskarten-Set inklusive gamifizierter Deep Dive-Workshop-Methode für Securityprofis und Manager, wird u. a. zur Visualisierung, Priorisierung und Planung von Security Awareness-Maßnahmen und zur Risiko-Betrachtung eingesetzt (s. a. „Gamification“, „Deep Dive-Workshop“ und Kap. 6.1 dieser Studie).

Assessment
Englisch für „Beurteilung“ oder „Bewertung“.

Audit
Untersucht im Rahmen von Qualitätsmanagement, ob Prozesse, Anforderungen und Richtlinien die geforderten Standards erfüllen.

Below the Line-Tools
Englisch für „unter der Linie“, abgekürzt BT. Steht im Marketing für alle „nicht-klassischen“ Werbe- bzw. Kommunikationsmaßnahmen (im Gegensatz zu sog. „Above-the-line-Maßnahmen“).

CEO-Fraud
Betrugsmasche des Social Engineering, bei der Organisationen unter Verwendung u. a. falscher Identitäten zur Überweisung von Geld manipuliert werden (s. a. „Social Engineering“, „Phishing“ und Kap. 6.3 dieser Studie).

Change
Englisch für „Veränderung“, im Kontext Change Management auch Veränderungsmanagement.

Change-Tools
Veränderungsinstrumente des Change Management.

Clean Desk bzw. Clear Desk
Informationssicherheitsstrategie eines „aufgeräumten“ Arbeitsplatzes, bzw. Büros im Sinne der Beachtung von Informationsklassifizierung, d. h. unter anderem sicheres Verschließen von Fenstern und Türen, Verschluss von sensiblen Informationen bzw. Wertsachen beim Verlassen von Arbeitsplatz resp. Büro (gilt i. d. R. auch für Meeting-Räume) usw. Dabei sind vor allem die Regeln einer Clean bzw. Clear Desk-Policy bzw. der Informationsklassifizierung zu beachten.

Coaching
Englisch von „to coach“ für „betreuen“, „trainieren“. Bezeichnet eine Vielzahl von Trainings- und Beratungskonzepten zur Entwicklung und Umsetzung persönlicher oder beruflicher Ziele und der dazu notwendigen Eigenschaften, in der Security Awareness häufig zur Ermächtigung bei Security Managern als begleitende Maßnahme von Kampagnen eingesetzt (s. a. „Supervision“ und Kap. 7.2 dieser Studie).

Compliance
Einhaltung aller gesetzlichen Bestimmungen durch Unternehmen und deren Mitarbeitenden.

Cover Story
Der nacherzählbare, vordergründige, offene, psychologische Stringenz liefernde Teil einer Geschichte, über die in der Kommunikation konkrete Informationen über Produkt, Service, Marke oder Inhalte an den Empfänger geliefert wird, in der Security Awareness z. B. die Kommunikation von Verhaltensregeln auf Basis von Richtlinien bzw. Policies [11] (s. a. „Impact Story“, „Storytelling“ und Kap. 1.5.5 dieser Studie).

Cyber Grooming
Gezielte Anbahnung sexueller Kontakte mit Kindern und Jugendlichen im Internet, u. a. auf Basis manipulativer Methoden (s. a. „Social Engineering“ und Kap. 5.7 dieser Studie).

Dax-30 Roundtable Security Awareness
Formloser Zusammenschluss der Verantwortlichen für Security Awareness in ausgewählten Dax-Unternehmen und vergleichbaren, größeren, in Deutschland ansässigen, meist international agierenden Organisationen mit dem Ziel des Austausches von Good Practices im Bereich Security Awareness. Gründungsteilnehmer waren u. a. T-Systems International, Bosch, Daimler, Lufthansa, Munich Re, RWE und Volkswagen. Heute gehören z. B. auch Deutsche Telekom, EnBW oder Kärcher dazu (s. a. Kap. 7.2 dieser Studie).

Deep Dive-Workshop
Workshop-Format und -Prozess – vor allem für Manager. In der Security Awareness u. a. zur Themenfindung und zur Priorisierung von Awareness-Maßnahmen (oder um Risiken zu visualisieren und zu evaluieren und in (Awareness-) Maßnahmen zu transformieren). Werden u .a. auf Basis des Moderationskartensets „askitMeta“ durchgeführt (s. a. „askitMeta“).

Diskursiv
Bildungssprachlich für „in ausführlichen Diskussionen, Erörterungen methodisch“ vorgehend.

DSGVO
Datenschutz-Grundverordnung, eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten EU-weit vereinheitlicht werden.

Edutainment
Kofferwort, das sich aus den englischen Wörtern „education“ (deutsch „Bildung“) und „entertainment“ (deutsch „Unterhaltung“) zusammensetzt und ein Konzept der elektronischen Wissensvermittlung zur Steigerung von Lernmotivation und -effizienz bezeichnet, bei dem die Inhalte spielerisch und gleichzeitig unterhaltsam vermittelt werden, z. B. über Web Based Trainings (WBTs) bzw. weitere interaktive Formate, z. B. steuerbare Videos oder Gamification.

Empowerment
Englisch für „Ermächtigung“, „Übertragung von Verantwortung“. Aus der Verhaltenstherapie abgeleitete Strategien und Maßnahmen, die den Grad an Autonomie von Einzelnen bzw. Organisationen erhöhen sollen und es ihnen ermöglichen, ihre Interessen eigenmächtig, selbstverantwortlich und selbstbestimmt zu vertreten. Empowerment bezeichnet dabei sowohl den Prozess der Selbstbemächtigung als auch die professionelle Unterstützung der Menschen, ihr Gefühl der Macht- und Einflusslosigkeit (powerlessness) zu überwinden und ihre Gestaltungsspielräume und Ressourcen wahrzunehmen und zu nutzen. Der Begriff wird auch für einen erreichten Zustand von Selbstverantwortung und Selbstbestimmung verwendet. In diesem Sinne wird im Deutschen Empowerment gelegentlich auch als Selbstkompetenz bezeichnet, die u. a. über Security Awareness-Maßnahmen erhöht werden soll. In der Informationssicherheit spielt Empowerment daher u. a. die Rolle, über Awareness-Maßnahmen persönliche Verantwortung gegenüber bzw. individuelle Mitgestaltung von Sicherheit zu kommunizieren und einüben zu lassen (s. a. Kap. 1.5.2 und 1.5.5 dieser Studie).

Face-to-face
Englisch für „im Angesicht“ bzw. „physisch präsent“.

Framework
Englisch für „Rahmenwerk“, d. h. schriftliche Grundlage für Management-Ordnungsstrukturen, um Programme, Initiativen, Kampagnen u. v. m. durchzuführen. Ein Security Awareness-Framework definiert u. a. langfristig Security Awareness-Methoden, -Ziele, -Instrumente und -Prozesse, die weit über das Konzept einer Einzelkampagne hinausgehen (s. a. Kap. 1.5 dieser Studie).

Gamification
Anwendung von Spieledesignprinzipien, -designdenken und -mechaniken auf (ursprünglich) spielfremde Anwendungen und Prozesse (s. a. „Serious Game“, „Planspiel“ und Kap. 5.1 dieser Studie).

Geolocation
Oft auch Geotargeting oder Geolokation genannt, ordnet IP-Adressen oder IPTC/XMP ihrer geografischen Herkunft zu.

Gestützt/ungestützt
Methode bei der Ermittlung eines Bekanntheitsgrads durch Interviews, z. B. im Rahmen von Recall-Tests in Bezug auf die kommunikative Gedächtniswirkung eines Probanden/einer Probandin. Gestützte Bekanntheit beschreibt mithin die Erinnerung durch Vorlage von Gedächtnisstützen(s. a. „Wirkungsforschung“ und Kap. 5 dieser Studie).

Giveaway
Englisch für „Werbeartikel“, „Werbegeschenk“. Ein Werbeträger, z. B. Streuartikel oder andere Gimmicks, den Unternehmen zum Zweck der Kommunikation „verschenken“. In der Security Awareness eingesetzt, um Sicherheitsveranstaltungen oder -botschaften stärker im Gedächtnis der Mitarbeitenden zu verankern – gerne auch am Arbeitsplatz (z. B. Tassen oder Kalender mit Awareness-Botschaften) (s. a. „Incentive“ und Kap. 5 dieser Studie).

Good Practice-Sharing
Teilen von bereits bewährten Methoden, Instrumenten u. ä. Ansätzen bzw. Inhalten (s. a. Kap. 5 dieser Studie).

Human Firewall
Englisch für „menschliche Brandmauer“. Betrachtet (achtsame) Mitarbeitende als sog. „last line of defense“, d. h. als die letzte „Verteidigungslinie“ vor einem Vorfall, und meint im Grunde die Verantwortung der Mitarbeiterschaft als Ganzheit hinsichtlich Informationssicherheit (s. a. Kap. 7.3 dieser Studie).

Impact-Story
Der unbewusst wahrgenommene, verdeckte, eine tragende Verfassung und ein motivrelevantes Fundament liefernde Teil einer Geschichte, über die in der Kommunikation implizite Informationen über Produkt, Service, Marke oder Inhalte geliefert werden – in der Security Awareness von hoher Wichtigkeit, um unbewusste Handlungen (z. B. Fehlleistungen) zu thematisieren[11] (s. a. „Cover Story“, „Storytelling“ und Kap. 1.5.5 dieser Studie).

Incentive
Von lateinisch „incentivus“ für „anregend“, „reizend“. Begriff der Werbesprache, der am besten mit „Anreiz“ übersetzt werden kann. Incentives können z. B. Geld- oder Sachprämien, Bonusprogramme (Reisen, Events), Lob bzw. Zertifikate für Mitarbeitende sein und werden im Bereich Security Awareness u. a. zur Belohnung bzw. Motivationsförderung eingesetzt (s. a. „Giveaway“ und Kap. 5 dieser Studie).

Incident Management
IT-Störungsmanagement, das typischerweise den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Betriebsstörungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse umfasst (s. a. „Security Incident“, „Reportingkultur“ und Kap. 3.5 dieser Studie).

Information Security Awareness
Teil einer umfassenden Sicherheitskommunikation, die gleichsam das Informationssicherheitsbewusstsein sowie den kompletten Sensibilisierungsprozess der Mitarbeitenden zum Thema „Informationssicherheit“ adressiert.

Informationsklassifizierung
Labeling von Informationen, die verschiedene Klassen hinsichtlich Berechtigungen auf Grundlage von Wert, Schadensausmaß bzw. Bedeutung der jeweiligen Information für die Organisation (s. a. Kap. 6.3 dieser Studie).

Information Security Management System (ISMS)
Verfahren und Regeln einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Integrierte Kommunikation
Prozess der allumfassenden und vernetzten, strategischen und damit zielgerichteten Kommunikation, die Analyse, Planung, Organisation, Durchführung und Kontrolle (auch Management) der gesamten internen und externen Kommunikation von Organisationen umfasst mit dem Ziel, eine konsistente, aufeinander abgestimmte Unternehmenskommunikation zu gewährleisten. In der Security Awareness wie auch in anderen Teilbereichen mithin die widerspruchsfreie Verknüpfung sämtlicher Kommunikationsinstrumente zu einer Ganzheit.

Involvement
Im angelsächsischen Wirtschaftsjargon „Einbezogenheit“, „Einbindung“. Im Marketing die Empfindung des Empfängers, dass ein Produkt, ein Service oder Inhalte etwas mit ihm selbst und seiner Persönlichkeit zu tun haben und eine Nutzung eine spürbare (positive) Auswirkung auf ihn zur Folge hat. Im Rahmen von Security Awareness von hoher Wichtigkeit, um Verantwortung gegenüber Sicherheit zu kommunizieren.

ISO 27001
Internationale Norm (Information technology – Security techniques – Information security management systems – Requirements), die die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und permanente Verbesserung eines dokumentierten ISMS unter Berücksichtigung des Organisationskontextes spezifiziert (s. a. Kap. 1.5.1 dieser Studie).

Key Performance Indicator (KPI)
Kennzahlen zur vergleichenden Analyse.

Key Visual
Englisch für „Schlüsselbild“, „Leitbild“, d. h. ein visuelles Grundmotiv, das die Positionierung einer Marke oder einer Organisation und einen langfristigen visuellen Auftritt prägt (s. a. „Security Branding“).

Kipplogik
Logik, die an der ambivalente Rezeption einer Kippfigur oder eines Kippbilds anknüpft.

KMU
Kleine und mittlere Unternehmen mit folgenden Begrenzungen: maximal 249 Mitarbeitende, jährlicher Umsatz höchstens 50 Millionen Euro, Bilanzsumme von höchstens 43 Millionen Euro [1].

Kognition
Informationsgestaltung bzw. -verarbeitung und insbesondere in der Psychologie die mentalen Prozesse (Denken, Lernen, Erinnern etc.) in Abgrenzung zu den emotionalen Prozessen (z. B. Fühlen, s. a. Kap. 1.5.5).

Kompetenzprofil
Gesamtheit aller Fähigkeiten auch der impliziten, nicht in Tätigkeitsprofilen beschriebenen (s. a. „Tätigkeitsprofil“ und „Sicherheitsprofil“).

Malware
Englisch für „Schadprogramm“ bzw. „Schadsoftware“ (s. a. Kap. 5.10 dieser Studie).

Mindfulness Based Stress Reduction (MBSR)
Achtsamkeitsbasierte Stressreduktion, ein Programm zur Stressbewältigung durch gezielte Lenkung von Aufmerksamkeit und durch Entwicklung, Einübung und Stabilisierung erweiterter Achtsamkeit, entwickelt von dem Molekularbiologen Jon Kabat-Zinn in den späten 1970er Jahren am Bostoner MIT, in Unternehmen in Deutschland z. B. seit vielen Jahren erfolgreich bei SAP eingesetzt. Im Rahmen von Security Awareness von ´zunehmend hoher Bedeutung, um Fehlleistungen der Mitarbeitenden durch ein intendiertes „Heraustreten aus dem Hamsterrad“ bzw. generell durch die Steigerung von Achtsamkeit zu vermeiden (s. a. Kap. 7.2 dieser Studie).

Morphologische Markt- und Medienpsychologie
Erfassung und Darstellung von Produkt- bzw. Medienverwendungsformen, Markenbildern oder generell Settings (z. B. Alltagssituationen) mithilfe von Tiefeninterviews und einer bestimmten Beschreibungs-, Analyse- und Transformationsmethode als lebendige Formenbildung [14] (s. a. „Wirkungsforschung“, „Qualitative Forschung“, „Tiefenpsychologie“ und Kap. 2 dieser Studie).

Narrativ
Sinnstiftende Erzählung, die per Modellierung hinsichtlich Kommunikation nutzbar gemacht wird (s. a. „Storytelling“).

Paradoxe Intervention
Psychologische, häufig in Therapie angewandte Methoden, die in scheinbarem Widerspruch zu ihren eigentlichen Zielen stehen, die aber tatsächlich zur Problemlösung entworfen sind. Informationssicherheit gilt generell infolge zahlreicher erlebter Widersprüche als ein paradoxes Thema. Ein Beispiel für eine paradoxe Intervention ist die sog. „Symptomverschreibung“, in der Security Awareness etwa über das Giveaway „Passworthalter“, ein Konzepthalter mit Karte, die dazu aufruft, sein Passwort zu notieren, bevor schließlich eine regelkonforme Richtigstellung erfolgt. Hierbei wird der Empfänger aufgefordert, in paradoxer Weise genau diejenige Situation herzustellen, die ihm Probleme bereitet. Dem liegt in der Security Awareness die Vorstellung zugrunde, auf diesem Weg einen Reflexionsprozessbezüglich des eigenen (Fehl-)Verhaltens anzustoßen (s. a. Kap. 5.12 dieser Studie).

Phishing
Neologismus abgeleitet von „fishing“, englisch für ‚Angeln“ bzw. in der Informationssicherheit Social Engineering via E-Mail mit den Versuchen, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben und dem Betrugsziel, an persönliche Daten von Internet-Usern zu gelangen oder diese zur Ausführung einer schädlichen Aktion zu motivieren (s. a. „Social Engineering“ und Kap. 6.2 und 6.3 dieser Studie).

Planspiel
Methode bzw. Instrument zur Simulation komplexer realer (soziotechnischer) Systeme, die häufig zu Lehr- und Lernzwecken und in der Awareness hinsichtlich der Vitalisierung und Emotionalisierung von Trainings und verwandter Formate eingesetzt werden (s. a. „Gamification“ und „Serious Game“).

Policies
Hier: Security Regelwerke.

Projektive Frage
Frage in Anlehnung an Projektion, Frage, die den psychoanalytischen Abwehrmechanismus adressiert. Der Begriff „Projektion“ umfasst das Übertragen und Verlagern innerpsychischer Inhalte oder eines innerpsychischen Konfliktes durch die Abbildung eigener Emotionen, Affekte, Wünsche, Impulse und Eigenschaften, die im Widerspruch zu eigenen und/oder gesellschaftlichen Normen stehen können, auf andere Personen, Menschengruppen, Lebewesen oder Objekte der Außenwelt. Die „Abwehr“ besteht dabei darin, dass durch Projektion vermieden wird, sich mit Inhalten bei sich selbst auseinanderzusetzen, die man beim anderen sieht (s. a. „Reaktanz“).

Qualitative Forschung
Sämtliche Erhebungen nicht standardisierter Daten und deren Auswertung auf Basis von u. a. interpretativen und hermeneutischen Methoden als Analysemittel, z. B. Wirkungsforschung (s. a. „Wirkungsforschung“, „Morphologische Markt- und Medienforschung“, „Tiefenpsychologie“ und Kap. 2 dieser Studie).

Quantitative Forschung
Sämtliche Methoden zur numerischen Darstellung empirischer Sachverhalte, z. B. via Fragebögen, aber auch zur Unterstützung der Schlussfolgerungen aus den empirischen Befunden mit Mitteln der Inferenzstatistik, u. a. Stichprobenauswahl, Datenerhebung und -analyse betreffend.

Reaktanz
Motivation zur Wiederherstellung eingeengter oder eliminierter Freiheitsspielräume, psychologisch häufig im Kontext seelischer Abwehr (z. B. Widerstand gegen umgebende Wirklichkeit) gebraucht (s. a. „Projektive Frage“).

Redundanz
Lateinisch von „redundare“ für „überlaufen, sich reichlich ergießen“. Beschreibt in der Informationstheorie diejenigen Informationen oder Daten, die in einer Informationsquelle mehrfach vorhanden sind.

Reportingkultur
Teil einer Sicherheitskultur, die das Security Incident Management mit seinem Meldewesen (Reporting) umfasst (s. a. „Incident Management“, „Security Incident“ und Kap. 3.5 dieser Studie).

Resilienz
Lateinisch von „resilire“ für „zurückspringen“, „abprallen“, eingedeutscht etwa „Widerstandsfähigkeit“. Beschreibt die Toleranz eines Systems gegenüber Störungen. Security Awareness soll u. a. die Resilienz der Organisation erhöhen (s. a. Kap. 1.1 und 6.1 dieser Studie).

Security Arena
Gamifiziertes Lernstationsformat der Awareness-Agentur known_sense, für Teams mit insgesamt 30 Informationssicherheits-, Datenschutz und Compliance-Themen, das weltweit lizenzierbar ist.

Security Branding
Markenführung der Sicherheitsbereiche in Organisationen als Teil von Sicherheitskommunikation, d. h. Aufbau und unter dramaturgischen Gesichtspunkten zu erfolgende Weiterentwicklung einer Sicherheitsmarke mit den Hauptzielen, den Wiedererkennungswert durch Kommunikation der charakteristischen Eigenschaften zu erhöhen sowie die eigene Leistung vom Angebot anderer Bereiche abzugrenzen und sich so über die eigenen Produkte, Dienstleistungen und Inhalte spürbar zu differenzieren und gleichzeitig Orientierung und Vertrauen bei der eigenen Zielgruppe zu schaffen. Security Branding umfasst u. a. ein Logo oder anderes Markenzeichen, Bildwelten mit Key Visuals, (Kern)Botschaften, Claim, Wording, Naming, Leitfigur(en), Narrativ(e) (s. a. „Key Visual“ und Kap. 1.5.4 dieser Studie).

Security Incident
Sicherheitsvorfall (s. a. „Incident Management“, „Reportingkultur“ und Kap. 3.5 dieser Studie).

Security Streetworking
Auf den Studien der Awareness-Agentur known_sense basierende Methode aus dem Security Awareness Manangement, das sich u. a. hinsichtlich der Kommunikation auf Augenhöhe mit der Zielgruppe (Mitarbeitende) begibt und einen intensiven Austausch mit diesen impliziert, Awareness mithin als eine Art „Sozialarbeit“ betrachtet.

Setting
Gesamtheit von Milieu, Umgebung, Situation, Bedingungen bzw. Arrangement, die den Rahmen von Erleben bildet (s. a. „Verfassung“).

Serious Game
Englisch für „ernsthaftes Spiel“. Digitales Spiel, das nicht primär oder ausschließlich der Unterhaltung dient, wohl aber derartige Elemente enthalten kann (s. a. „Gamification“, „Planspiel“ und Kap. 7.2 dieser Studie).

Sicherheitskultur
Gesamtheit der Überzeugungen und Werte von Individuen und Organisationen, bei denen eine Übereinkunft herrscht, welche Ereignisse Risiken darstellen bzw. mit welchen Mitteln diesen Risiken strategisch begegnet wird [5] (s. a. Kap. 1.5.4 dieser Studie).

Sicherheitsprofil
Addition von sicherheitsrelevanten Skills sowie Zutritts- bzw. Zugriffsrechten (s. a. „Kompetenzprofil“ und „Tätigkeitsprofil).

Social Engineering
Form der Manipulation, bei der ein Angreifer unter Verwendung gesammelter Informationen und/oder Vortäuschung falscher Tatsachen versucht, unberechtigten Zugang zu vertraulichen Informationen oder IT-Systemen zu erlangen (s. a. Kap. 5.8 dieser Studie).

Stationenlernen
Lernmethode, bei der die Lernenden in der Regel selbst gesteuert bzw. eigentätig, optional auch teamorientiert anhand vorbereiteter Materialien bzw. auf Basis einer Moderation, deren Themen in Stationen angeordnet sind, mit möglichst vielen beteiligten Sinnen lernen, z. B. mithilfe der „Security Arena“.

State-of-the-art-Awareness
Stand bzw. Reifegrad jeweils aktueller Security Awareness-Maßnahmen.

Storytelling
Englisch für „Geschichten erzählen“. Eine für den Erfolg von Awareness wichtige narrative Methode, bei der explizites, aber vor allem implizites Wissen in Form von Metaphern weitergegeben wird. Die Zuhörenden werden in die Geschichten eingebunden, damit sie den Gehalt leichter verstehen und mitdenken mit dem Ziel, die Inhalte besser und schneller aufzunehmen, nachhaltiger zu memorieren und eigenständig anzuwenden (s. a. „Narrativ“ und Kap. 1.5.5 dieser Studie).

Supervision
Lateinisch für „Über-Blick“. Qualifizierungsform für Mitarbeitende mit dem Ziel, Rollen- und Beziehungsdynamik sowie die Zusammenarbeit in Teams und Organisationen zu reflektieren und zu verbessern – in der Security Awareness vor allem für Führungskräfte und Security-Teams (s. a. „Coaching“ und Kap. 7.2 dieser Studie).

Systemische Kommunikation
Für Awareness-Prozesse und insbesondere Ebene 3 (Können) relevantes Modell des Kommunikationsforschers Paul Watzlawick auf der Grundlage, dass Kommunikation stets abhängig von der Beziehung der Teilnehmenden ist und es im zwischenmenschlichen Bereich unmöglich sei, nicht zu kommunizieren. Dies bedeutet für Security Awareness, dass z. B. jede wahrnehmbare Aktion eines Securityprofis bereits Teil seiner Sicherheitskommunikation und damit auch von Security Awareness ist (s. a. Kap. 1.5.5 dieser Studie).

Tätigkeitsprofil
Offizielle, vom Arbeitgeber veranlasste Beschreibung mit einer Tätigkeit verbundenen Aufgaben bzw. Erwartungen (s. a. „Kompetenzprofil“ und „Sicherheitsprofil“).

Tiefeninterview
Beim psychologischen Tiefeninterview wird im Rahmen eines sich verdichtenden Kommunikationsprozesses so vertiefend evaluiert, bis die psychologische Wurzel eines Phänomens zu erkennen und zu beschreiben ist (s. a. „Tiefenpsychologie“ und Kap. 2 dieser Studie).

Tiefenpsychologie
Ausgehend von der der Philosophie (Leibniz, Schopenhauer, Nietzsche) und Sigmund Freuds Psychoanalyse, Oberbegriff für sämtliche psychologische Ansätze, die unbewusste seelische Vorgänge als Erklärung menschlichen Verhaltens und Erlebens betrachten, bei denen „unter der Oberfläche“ des Bewusstseins unbewusste Prozesse ablaufen, die das bewusste Seelenleben stark beeinflussen. Relevanz für Security Awareness vor allem in der Erklärung unbewussten Mitarbeiterverhaltens im Kontext von Fehlerkultur bzw. mangelnder Compliance, aber auch hinsichtlich der Kommunikation, z. B. bei der Ausgestaltung der Impact Story [11] (s. a. „Wirkungsforschung“, „Qualitative Forschung“, „Tiefeninterview“ und Kap. 2 dieser Studie).

Train-the-trainer
Methode für Business-Trainings, bei der Experten/Expertinnen dazu befähigen, ebenfalls als Experte/Expertin (Trainer/in, Moderator/in, Supervisor/in u. ä.) tätig zu sein.

Verfassung
Stimmung, Zustand bzw. (psychologische) Bedingungen, in denen sich Menschen (exakter: Empfänger/innen) befinden, die mit bestimmten Kommunikationsmaßnahmen in Kontakt kommen. Auch Grundlage des sog. Verfassungsmarketings, das sich vom Zielgruppen-Marketing abgrenzt. Beispielsweise unterscheiden sich Wochenend-Verfassungen der Mitarbeitenden an Freitagen erheblich von den Wochenstarts an Montagen und erzeugen so unterschiedliche Stimmungswelten, die auch für den Einsatz von Medien und Kanälen relevant sind (s. a. „Setting“ und Kap. 2 dieser Studie).

Virales Marketing
Marketingform, häufig auch „Guerilla Marketing“ genannt, die überwiegend soziale Netzwerke bzw. Medien oder Live-Aktionen nutzt, um Aufmerksamkeit über i. d. R. ungewöhnliche bzw. hintergründige Inhalte zu erzeugen.

White-Hat-Hacker
Ethische Hacker und Informationssicherheitsexperten und -expertinnen, die u. a. mithilfe von Hacking-Tools und -Methoden IT-Systeme testen und Sicherheitslücken aufdecken, damit Organisationen ihre Systeme besser schützen können.

Wirkungsforschung
Überwiegend psychologische Forschung, die nicht singuläre Phänomene, sondern den ganzheitlichen Zusammenhang (vollständige Bilder, Unbewusstes, Motivationen und Entscheidungsprozesse) analysiert und beschreibt (s. a. „Morphologische Markt- und Medienforschung“, „Qualitative Forschung“, „Tiefenpsychologie“ und Kap. 2 dieser Studie).

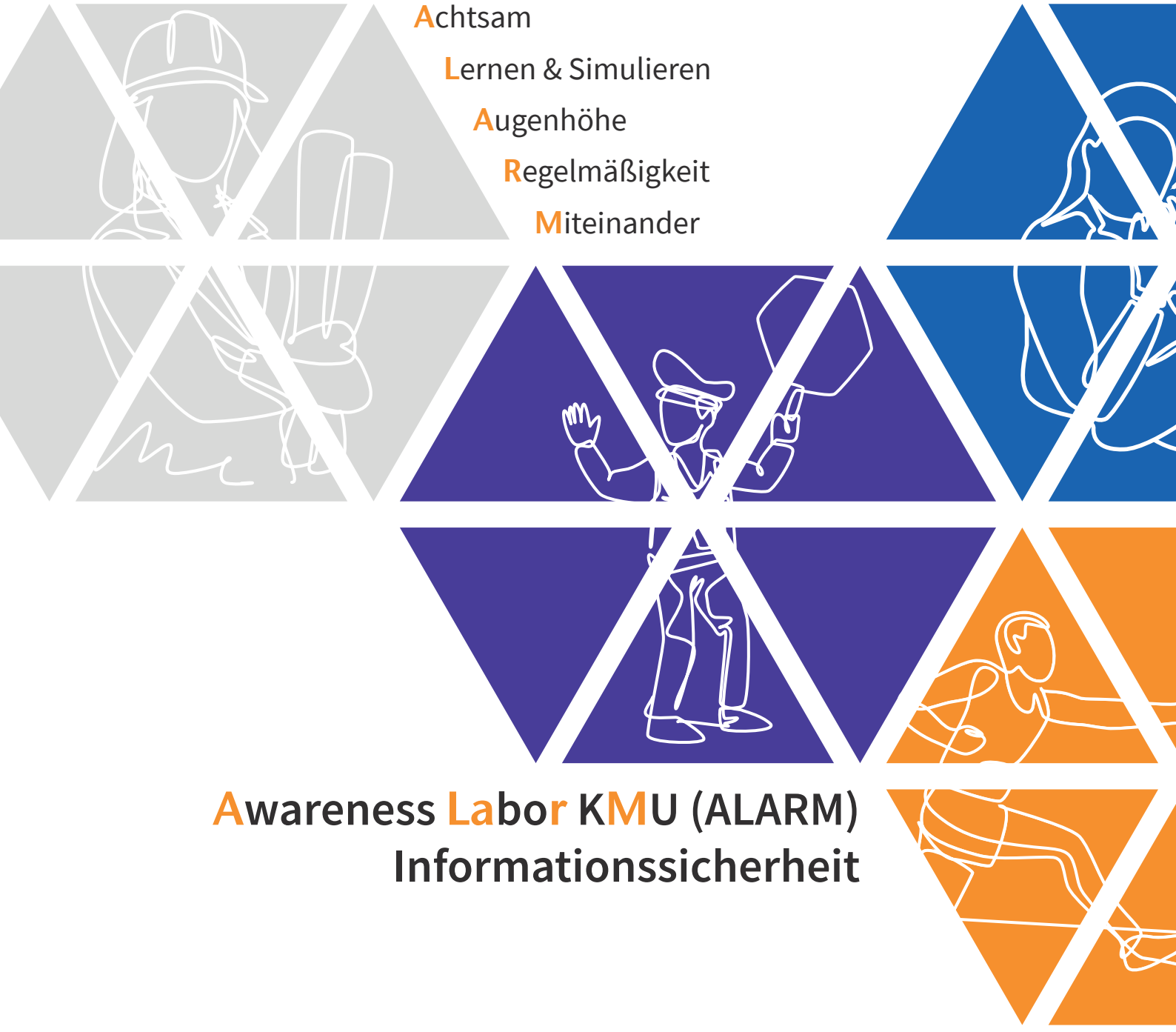
Wording
Bereitstellung eines Katalogs an Euphemismen (lateinisch für „Worte von guter Vorbedeutung“; auch „Beschönigung“ oder „Verbrämung“), deren Nutzung im Rahmen von Kommunikationsmaßnahmen den Aufbau eines stimmigen, konsistenten Bildes der kommunizierten Inhalte fördern soll. In der Sicherheitskommunikation von hoher Wichtigkeit, um Konsistenz herzustellen (s. a. „Security Branding“).

Zielgruppe
Im Marketing und auch hinsichtlich Security Awareness eine definierte Teilmenge aller anzusprechenden Personen (exakter: Empfänger/innen), die auf kommunikative Maßnahmen homogener reagieren als die Gesamtmenge. Basis der Zielgruppendefinition ist eine Segmentierung nach jeweils relevanten Gesichtspunkten.

Technische Hochschule Wildau
Technical University of Applied Sciences

known_sense
awareness you can touch.

Achtsam
Lernen & Simulieren
Augenhöhe
Regelmäßigkeit
Miteinander



Awareness Labor KMU (ALARM)
Informationssicherheit

ISBN 978-3-949639-00-5