TAKE AWARE

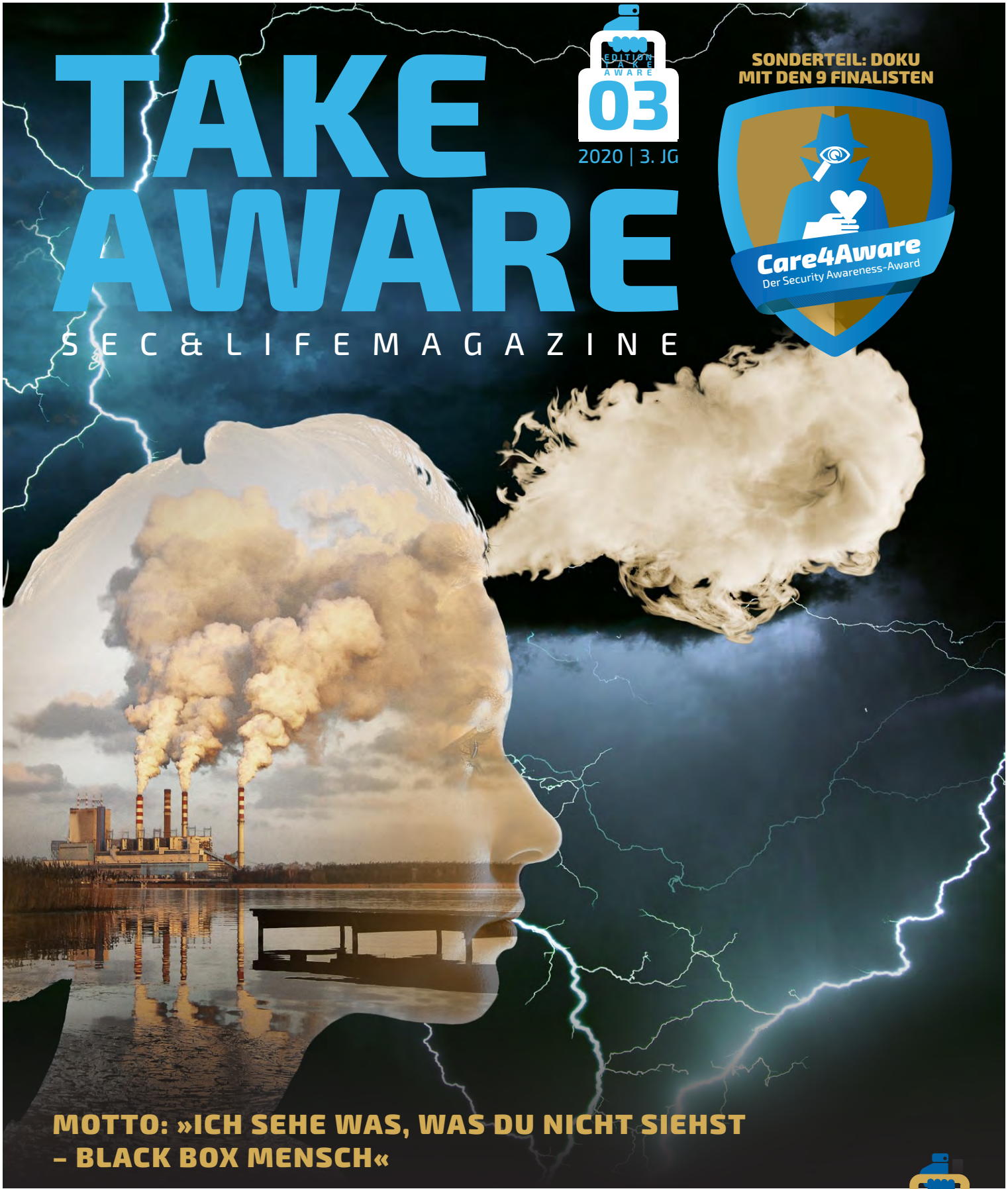
SEC&LIFEMAGAZINE

EDITION TAKE AWARE 03

2020 | 3. JG

SONDERTEIL: DOKU MIT DEN 9 FINALISTEN

Care4Aware
Der Security Awareness-Award



MOTTO: »ICH SEHE WAS, WAS DU NICHT SIEHST – BLACK BOX MENSCH«

DIE BESTEN MASSNAHMEN – CARE4AWARE-FINALISTEN | DIE BESTEN MAIL-SIMULATIONEN – ELEVATOR-PITCH PHISHING | DIE BESTE REGEL-SENSIBILISIERUNG – DER COMPLIANCE PARCOURS | WECKE DEN SPIEL-TRIEB – LERNEN MIT ACTIONBOUND | AWARENESS GANZ OHNE SENSIBILISIERUNG: MBSR – MINDFULNESS BASED SECURE REACTION

TAKE AWARE
Die Security AwarenessKonferenz
www.take-aware.com

EIN EVENT DER TAKE AWARE
SEXY SECURITY
SECURITY BRANDING & CREATIVE CAMP
www.take-aware.com

Herausgegeben von

my breev

known_sense
awareness you can touch.

Medienpartner

CORPORATE-SECURITY.TV


STAY at
HOME

TAKE AWARE SEC&LIFEMAGAZINE 03

STAY AT HOME! (AUSSER DIE TAKE AWARE RUFT)

Liebe TAKE AWARE-/SEXY-SECURITY-Bucher, verehrte Awareness-Freunde,

die 3. Ausgabe unseres Magazins, das erstmal ausschließlich digital erscheint, drängt sich mit einer fünfmonatigen Verspätung in Ihren Arbeitsalltag – zu spät nicht etwa, weil es zum kalkulierten Erscheinungstermin Mitte März noch nicht lesefertig gewesen wäre, sondern weil in diesem „Wendejahr" 2020 die Seuche förmlich an allem klebt, dem das Etikett der Live-Kommunikation anhaftet. Denn wie schon in den letzten Jahren sollte das Magazin anlässlich eines unserer TAKE AWARE EVENTS – in diesem Fall zur 4. Awareness-Doppelkonferenz – diesmal im Stuttgarter Innenministerium – erscheinen. Aber COVID-19 hat uns wie so vielen anderen Kollegen das lange und liebevoll vorbereite Event verhagelt. Da einige Tage vor der TAKE AWARE im Gottlieb-Daimler-Stadion noch ein Fußballspiel vor knapp 50.000 Zuschauern stattfand, taten wir uns zugegebenermaßen sehr schwer mit der kurzfristigen Absage – aber das Virus und die damit verbundenen Maßnahmen haben uns keine andere Wahl gelassen. Mit der Absage des Events hatten wir auch entschieden, die Publikation des Magazins auszusetzen, bis sich gegebenenfalls ein Lichtstreif am Horizont abzeichnen würde. Jetzt nach fünf Monaten können wir konstatieren, dass es in 2020 definitiv keine TAKE AWARE und SEXY SECURITY mehr geben wird. Nicht in Stuttgart. Nicht anderswo in Deutschland. Zwar wären Veranstaltungen unserer Größenordnung juristisch lupenrein in einigen Bundesländern durchzuführen; aber was nützt es uns, wenn wir veranstalten dürfen und aber am Ende alleine dort sitzen, weil z. B. Sie aufgrund von Reisebeschränkungen gar nicht kommen dürfen. Die 2020er Doppelkonferenz wird also nach heutigem Stand frühestens wieder im Frühjahr oder Frühsommer 2021 stattfinden. Als kleine Überbrückung schenken wir Ihnen aber hiermit zumindest unser im März ebenfalls aufgeschobenes Magazin in der Hoffnung, dass Security Awareness weiterhin Thema für Sie und Ihre Organisation bleibt – auch in diesen schwierigen Zeiten – und Sie uns als Teilnehmer unserer Events erhalten bleiben. In der Zwischenzeit heißt es zwar „Stay at home", wir würden uns aber freuen, Sie 2021 tatsächlich wieder live bei uns begrüßen zu dürfen. Die traditionellen T-Shirts für alle SEXY SECURITY-Bucher warten dann mit dem Motiv auf S. 31 auf Sie. Und dann wird sich auch das Geheimnis lüften, welche Finalisten aus der Shortlist auf den S. 10-19 mit den drei begehrten Care4Aware-Trophäen ausgezeichnet werden.

TAKE AWARE. TAKE AWAY. TAKE CARE.

Dietmar Pokoyski & Uwe Röniger, Herausgeber TAKE AWARE seco-life magazine

CONTENT

Das TAKE AWARE SEC&LIFE MAGAZINE wird herausgegeben in der EDITION TAKE AWARE von den TAKE AWARE EVENTS mit den Partnern known_sense & mybreev GmbH | Redaktion: Dietmar Pokoyski & Uwe Röniger | Layout: known_sense | Kontakt & Anzeigen mybreev GmbH | Bahnhofstraße 1c | 41747 Viersen | Fon 02162 1065549 | info@mybreev.com | www.take-aware-events.com

Abbildungen: S. 1 (Titel),2, 4, 6, 9, 20,24, 32 (Titel) Shutterstock | S. 7, 8, 10, 31 known_sense | S. 11-19 einzelne Care4Aware-Bewerber | S. 23 Realfiction | S. 25 mybreev bzw. BSI | S. 30 einzelne Autoren

WECKE DEN SPIELTRIEB: LERNEN MIT GAMIFICATION

VON LOTTA KRICKEL & MARCUS BEYER

Was ist Gamification? Kurz erklärt, bedeutet Gamification, dass man einen Lerninhalt mit spielerischen Elementen versieht, um so die Motivation und den Lernerfolg zu steigern. Immer häufiger wird Gamification in Unternehmen z. B. zur Weiterbildung eingesetzt.

Wir alle kennen Spiele. Denn jeder Mensch hat schon einmal gespielt. Als kleine Kinder legt das entdeckende Spielen ohne Regeln und Ziele die Basis für die psychosoziale und kognitive Entwicklung. Später erlernen wir durch zielgerichtete Spiele unterschiedlichste Kompetenzen – von sozialen Fähigkeiten wie Frustrationstoleranz und Teamfähigkeit bis hin zu Hardskills wie z. B. das Zählen oder Rechnen. Im Englischen unterscheidet man daher zwischen „Play", also dem unspezifischen Spiel, und „Game", dem Spielen in einem bestimmten Rahmen.

Eine der wichtigsten Voraussetzungen für das Spielen ist Freiwilligkeit. Spielen soll Spaß machen! Ein Spiel zu spielen, ist in der Regel keinem anderen Zweck unterworfen, als ein spaßiger Zeitvertreib zu sein. Die Herausforderung ist, Lust am Spielen zu wecken. Die Frage, die sich jeder Spieleentwickler stellen muss, ist: Wie kann mein Spiel Spaß machen? Punkte vergeben, einen Sieger küren und lustige Sounds als Feedback, fertig ist das interaktive Spiel – oder? Ganz so einfach ist es dann aber doch nicht. Um einen nachhaltigen Lernerfolg zu erreichen und Spieler*innen ein positives Gefühl zu vermitteln, bedarf es ein wenig mehr.

Zum Glück haben schon viele diese Frage vor uns beantwortet und wir müssen das Rad nicht komplett neu erfinden. Hier hilft es, sich an Videospielen zu orientieren. Nicht umsonst ist die Gaming-Industrie die erfolgreichste Entertainmentbranche der Welt. Wenn auch wir erfolgreich Gamification nutzen möchten, müssen wir weiterdenken als nur an spielerische Elemente. Wir müssen uns mit dem gesamten Konzept eines Spiels, dem Game Design, beschäftigen.

Game Design mit Storytelling

Game Design beschreibt die komplette Entwicklung eines Spiels inklusive der Story, Charaktere, Grafik, Gameplay usw. Um ein Gefühl für Game Design zu bekommen, ist es hilfreich, sich erfolgreiche Games, insbesondere solche, die Storytelling nutzen, genauer anzuschauen. Aber nicht nur digitale Spiele können erfolgreiches Game Design aufweisen. Im analogen Raum sind es elaborierte Storytelling Games wie Escape Rooms oder Exit-Spiele, die Anregungen für Lernspiele geben können.

Für die praktische, pragmatische Umsetzung von Gamification bietet sich unter anderem die Software von Actionbound an, mit der sich vom einfach Quiz bis hin zur digital geführten Schnitzeljagd ohne vertiefende Vorkenntnisse verschiedene Lernspiele entwickeln und per App spielen lassen.

Scavenger Hunts oder Virtuelle Schnitzeljagden

Das Team von Marcus Beyer (DXC Technolgy) hat den Einsatz von Actionbound in Security Awareness Kampagnen erfolgreich ausprobiert. Dies erfordert Mut – oder den Wunsch nach etwas Besonderem bzw. Ausgefallenem. Denn das ganze Thema „Gamification" erscheint vielen Organisationen so „neu", dass es in der internen Kommunikation oder in den Bereichen Ausbildung, IT- bzw. Informationssicherheit gerade erst ankommt. Ob es Zurückhaltung oder das vermeintlich Neue ist – zunächst werden meist aufwendige Diskussionen um die Rahmenbedingungen geführt: Muss man Leihgeräte zur Verfügung stellen? Wie kann man das Management davon überzeugen, dass man ihre Mitarbeitenden auf eine Schnitzeljagd schickt und keine klassische Frontalschulung bzw. E-Learnings anbietet (oder dies sogar noch zusätzlich implementiert)? Wie lange darf so eine Schnitzeljagd überhaupt dauern, – etwa länger als 15 Minuten(?) – um nur einige Ansätze bezüglich des Diskussionsbedarfs zu nennen.

Emotionalisierung von Informationssicherheit

Grundsätzlich sollte jedoch eines klar sein – ob „Cyber Security Hero Challenge" oder „Sicherheitsschatzsuche" – es wird gespielt. Es MUSS gespielt werden! Nichts ist langweiliger, als Wissensfragen aus einem E-Learning in ein Spiel zu portieren. Im Gegensatz dazu können physisch-analoge Umgebung sowie spannende, narrative Aufgaben und Rätsel eine Sicherheitsschulung zu einem echten Erlebnis machen. Natürlich ist die Entwicklung eines gut durchdachten, auf einer Story basierenden, multimedialen und interaktiven Spiels aufwendig, aber es funktioniert – und es lohnt sich!

Mut, Lernprozesse „anders", spielerisch anzugehen, zahlt auf die Emotionalisierung des Themas Informationssicherheit ein. Und das ist ja genau das, was wir in unseren Security Awareness-Kampagnen anstreben. Die Nutzung von Actionbound ist eine sehr gute Idee für einen zusätzlichen, neuen Kommunikationskanal. Und den muss man nun erstmal für sich entdecken.

*Actionbound ist eine Software, mit der multimediale, digitale Lernrallyes erstellt und per App gespielt werden können. Die sogenannten Bounds können im browserbasierten Web Editor ("Bound-Creator") nach einem Baukastenprinzip kombiniert und mit Inhalt gefüllt werden. Neben der Software bietet Actionbound auch Workshops und individuelle Consultings zu Gamification, Game Design und Storytelling an. 2012 von Simon Zwick und Jonathan Rauprich gegründet, wurde Actionbound zunächst vor allem im Bildungsbereich als moderne digitale Lern- und Lehrmethode eingesetzt. Mittlerweile zählt Actionbound namhafte Kunden wie Fraport, Allianz, Pfizer und viele weitere zu ihren Nutzer*innen.*

BE AN ALLIANCE IN COMPLIANCE!

GEMEINSAM SPIELERISCH ZUR COMPLIANCE-AWARENESS

VON JEAN KOLAROW

Das Thema Compliance hat in den letzten Jahren zunehmende Aufmerksamkeit erfahren und erhielt im Zuge der in den Medien aufgearbeiteten Vorfälle innerhalb diverser Konzerne und anderer Organisationen den Status eines Qualitätsmerkmals – nicht allein bezüglich einwandfreien Unternehmensverhaltens in der öffentlichen Wahrnehmung, sondern gleichermaßen als strategisches Mittel der regelkonformen Unternehmensführung.

Trotz dieser jüngsten Entwicklungen wird Compliance oftmals mit bloßer Regulierung, Überwachung, Kontrolle und auch Sanktionen in Verbindung gebracht; zusammenfassend also als Maßnahme, die von oben herab diktiert und unter hohem Aufwand an personellen und organisatorischen Ressourcen als ethisch-moralisches Scheinkonstrukt angesehen oder – unter dem Deckmantel der so genannten Corporate Social Responsability – als Selbstdarstellungs-Instrument mit hoher Außenwirkung wahrgenommen wird.

Gründe für diese Haltung sind oftmals Verständnisschwierigkeiten der Betroffenen bzw. Verpflichteten zu Zweck und Zielstellung von Compliance. Dass diese nicht als Good-Will-Redundanz, sondern als nachhaltige Maßnahme der Unternehmenslenkung dient und über Erhalt oder Untergang eines Unternehmens entscheiden kann, erscheint den Wenigsten bewusst. Compliance stellt sich zudem in erster Linie nicht als Rechtsproblem, sondern als Kommunikationsproblem dar. Ihre Grundlagen sind unbestritten Gegenstand rechtlichen Regelungsgehalts. Die tatsächliche, praktische Umsetzung zielt jedoch auf die Verhaltensweisen der Beschäftigten eines Unternehmens ab. Die entsprechenden Regelungsinhalte müssen demnach deren Motivation, Wahrnehmung und ebenso ihren Kompetenzen kognitiv sowie ideell zugänglich gemacht werden. Statt eines Betriebslebens in der bloßen Papierlage diverser Regulationen muss allen klar sein, dass sie Teil eines Compliance-Hive-Bewusstseins sind, an dem alle aktiv mitwirken können und sollen. Dies zu erreichen muss daher als Königsdisziplin unter den Compliance-Schaffenden verstanden werden. In ihrer Verantwortung liegt folglich gleichermaßen die Übersetzung des unverständlich juristischen Paragraphen-Sprechs in die spezifische Sprache aller Beschäftigten des Unternehmens.

Leichterer Zugang über Gamification

Der Compliance Parcours bedient sich dafür des Prinzips der sogenannten „Gamification“ und verschafft den Teilnehmenden den Zugang zu theoretischen Inhalten mithilfe spielerischer Vermittlungsmethoden. Was zunächst ein wenig waldorfisch anmuten mag, bedient sich wissenschaftlich fundierter Erkenntnisse aus dem Bereich der Lernpsychologie. Die verfügbaren Stationen zielen auf das Lernen in Kleingruppen ab und bieten so bezüglich Interaktion, Diskussion und Auseinandersetzung über ein Thema auf sozialer Ebene einen wesentlichen Vorteil gegenüber digitalen Lösungen, deren Pixelwelt letztendlich nur die nervtötende Abarbeitung an sich selbst zulässt. Soziale Interaktion durch diskursive Didaktik ist dabei kein kurzlebiges Buzzword eines neu gehypten Trends, sondern eine seit Jahrzehnten verbreitete

Der Compliance-Parcours bietet bisher Lernstationen zu folgende Themen an:

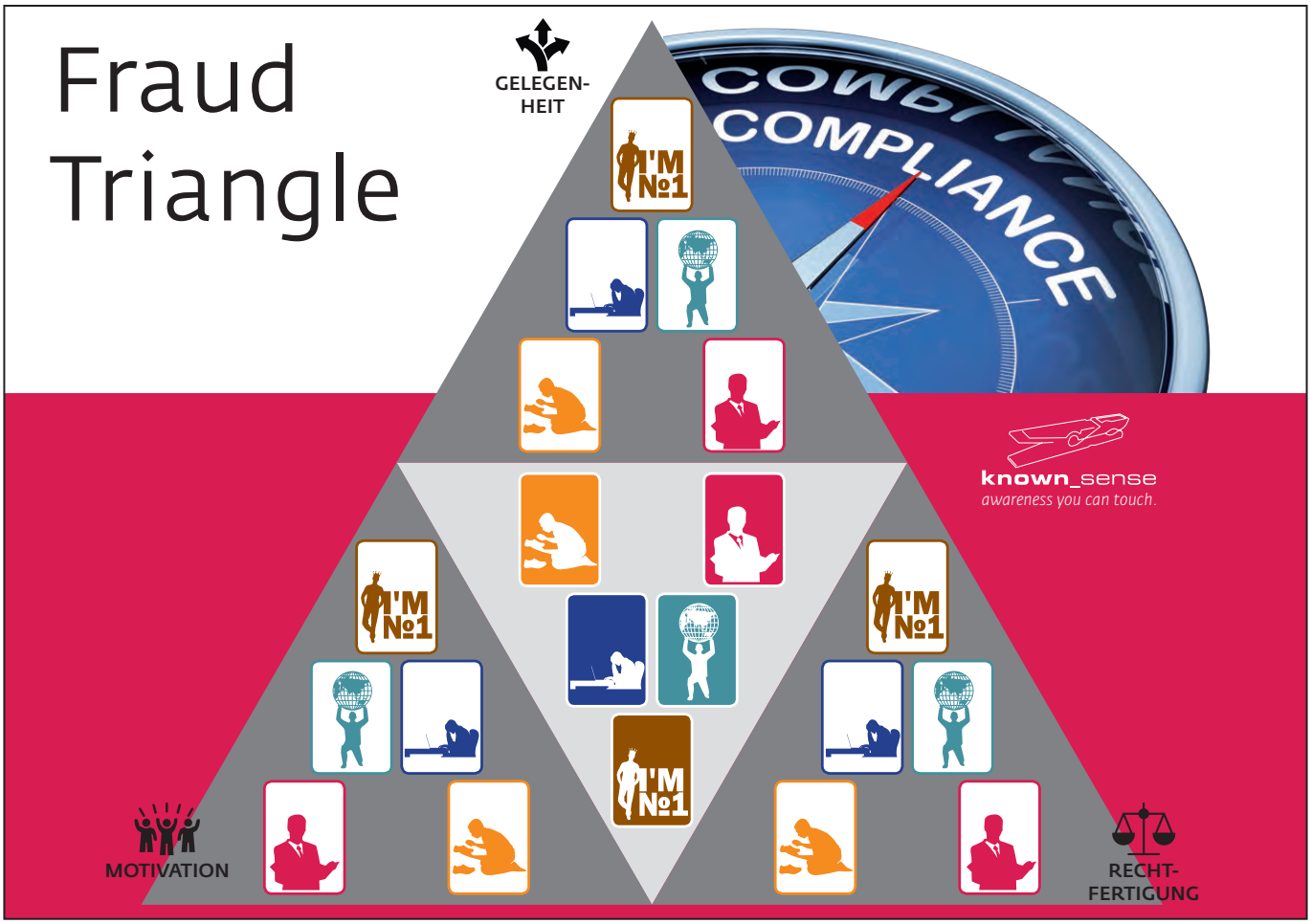
1. Compliance in Gesetzen
2. Definition des Compliance-Begriffs
3. Die Compliance-Organisation
4. Die Three Lines of Defense
5. Korruption
6. Risikomanagement
7. Non-Compliance-Schäden
8. Das Fraud Triangle
9. Annahme von Zuwendungen
10. Der Compliance-Vorfall

Erkenntnis. Sie erzeugt aktive Diskussionen und Austausch untereinander, statt gähnende Langeweile und Kopfschütteln über die gestohlene Lebenszeit.

Für kleine und große Unternehmen

Das Themenportfolio wird stetig erweitert bzw. für Kunden neu kreiert und verstärkt somit die Security Arena von known_sense um das Thema Compliance. Der Parcours ist für Unternehmensgrößen aller Art geeignet und kann sowohl zum Einsatz

Annahme von Zuwendungen



Der vorliegende Artikel basiert auf der Jean Kolarows Masterthesis „Entwicklung eines analogen Lernformates für die Schulung von Compliance-Inhalten unter Berücksichtigung lernpsychologischer Faktoren" an der Rheinischen Fachhochschule Köln. Die finale Produktentwicklung wurde gemeinsam von Kolarow und dem Gamification-Experten Dietmar Pokoyski von der Awareness-Agentur known_sense vorgenommen, die diese Lernstationen bzw. den kompletten Parcours auch individuell adaptiert und im Branding der jeweiligen Kunden weiterlizenziert. Weitere Informationen bzw. die Preisliste via known_sense (sense@known-sense.de).

kommen, um Beschäftigte erstmalig an das Thema Compliance heranzuführen, als auch bei Wiederholungsausbildungen angewendet werden. Zudem ist er geeignet, um das in einem Compliance Management-System geforderte Awareness-Building im Rahmen eines Audits oder einer Zertifizierung nachzuweisen. Deshalb muss auch für ihr Unternehmen gelten: Be an Alliance in Compliance!

Hintergrund: Die Informationssicherheits-Lernstationen der Security Arena

Bei der Security Arena, dem Vorbild des Compliance Parcours, durchlaufen Teams mit 3 bis 12 Teilnehmern synchron 4-6 Themenstationen, an denen sie von Moderatoren hinsichtlich verschiedener Sicherheits-Themen sensibilisiert werden.

Jede der derzeit 18 angebotenen Informationssicherheits-Stationen dauert lediglich 15 Minuten und beinhaltet u. a. jeweils ein „Minigame", das mit den anderen Games und Moderatoren-Briefings in einen handelsüblichen Koffer passt. Moderiert wird stets von Kollegen (d. h. „Laien") auf Basis eines Train-the-Trainer-Konzepts. An jeder Station können die Teams Punkte sammeln und am Ende einen Teampreis gewinnen. Nach jeweils 15 Minuten und den stets identischen drei Phasen (Einleitung – Minigame – Debriefing) wird die Station gewechselt. So können während eines Sicherheits-Event täglich bis zu 350 Mitarbeiter mit Brennpunktrisiken und deren Abwehr vertraut gemacht werden.

Die Security Arena hat sich seit 2011 an in 30 Ländern auf allen 5 Kontinenten bewährt – von Brasilien bis Australien, von Südafrika bis nach Russland. 2013 wurde der Arena-Line-Extender „SECURITY PARCOURS" vom ISF (International Security Forum) als weltweit „innovativste Awareness-Kampagne" ausgezeichnet. 2015 erhielten known_sense und die Security Arena den OSPA (Outstanding Security Performance Award, Kategorie „Herausragende Initiative für Sicherheitsschulungen").

Security Arenen werden bei den Lizenznehmern in der Regel lokal organisiert, wobei jede Einheit ihr Arena-Event unabhängig mit angepassten Inhalten, eigenen Moderatoren und eigenen Marketingmitteln durchführt. known_sense stellt mit dem zentralen Sicherheitsmanagement jedes Kunden Methoden, (didaktischen) Content und Event-Support als Unterstützung des lokalen Sicherheitsmanagements zur Verfügung. Das komplette Material für alle Stationen samt dazugehörigem Supportmaterial (z. B. Promotion- oder Themenposter, diverse Event-Organisations-Templates) passt in einen handelsüblichen Koffer – eine Roadshow ‚out of the box'!

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

CARE4AWARE

DER NEUE SECURITY AWARENESS-AWARD

VON MICHAEL HELISCH & DIETMAR POKOYSKI

Erstmals in der Geschichte der TAKE AWARE/SEXY SECURITY werden von den TAKE AWARE EVENTS in Zusammenarbeit mit HECOM Security Awarenss Consulting und unter der Marke „Care4Aware“ die besten Security Awareness-Initiativen der vergangenen Dekade im deutschsprachigen Raum ausgezeichnet. Der Wettbewerb richtete sich sowohl an Unternehmen aus der Privatwirtschaft wie auch an öffentliche bzw. nicht-kommerzielle Träger, nicht aber an Dienstleister wie Agenturen, Beratungsunternehmen oder Anbieter von Tools. Die Prämierung der besten drei Wettbewerbseinreichungen erfolgt durch eine Expertenjury (Dr. Katja Dörlemann/SWITCH, Prof. Dr. Angela Sasse /Ruhr-Universität Bochum, Michael Lardschneider/Munich Re, Wolfgang Reibenspies/ Ex-EnBW, Nina Malchus/me – malchus eventmanagement, Stefano Merenda & Ulrike Albanese/Propella) und berücksichtigt drei Kategorien:

1. PROMOTE: Bestes Security Branding (Kombination der Kampagnenelemente Logo, Key Visuals, Logo, Claim, Naming, Wording etc.)
2. PERFORM: Beste (kurzfristige) Security Awareness-Kampagne
3. CHANGE: Bestes (mittel- bis langfristiges) Security Awareness-Programm

Care4Aware: Nominiert in der Kategorie PROMOTE:
AMAG Corporate Services AG: „Information Security – more than IT“ (2019 ff.)

«Information Security – more than IT»

» Mit dem Claim „Information Security – more than IT“ schaffen wir Wiedererkennung und erklären gleichzeitig, dass sich die Informationssicherheit nicht nur auf die Informatik beschränkt, sondern dass es auch um die physische Sicherheit von Daten geht.

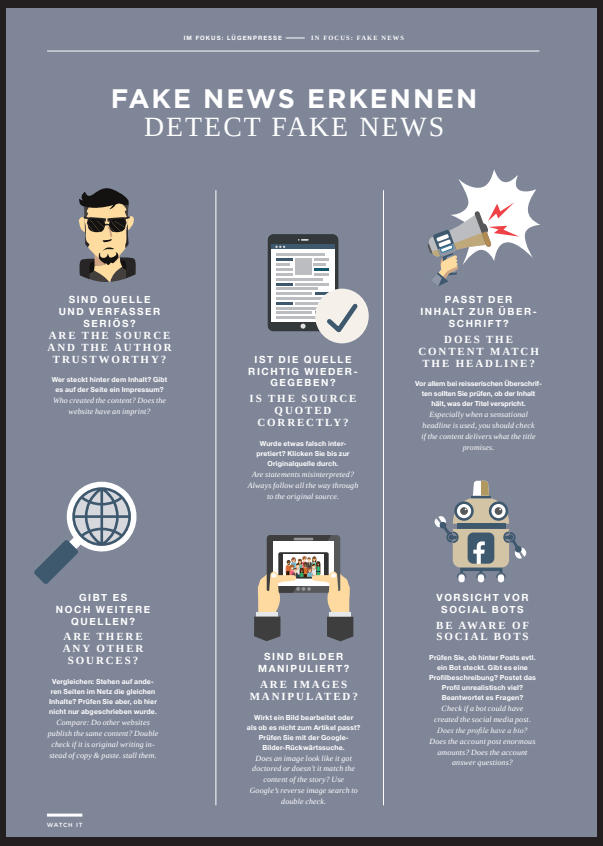
Dies zu vermitteln, ist in einem Unternehmen wie der AMAG, in dem mehr als 45% Mitarbeitende nicht am Laptop arbeiten, enorm wichtig.

Mit dem Key Visual Troy schaffen wir Wiedererkennung und eine einzigartige Möglichkeit, Botschaften auf eine spielerische und verständliche Art zu vermitteln.

Troy hilft uns mit seiner Anwesenheit, unsere Mitarbeitenden auf die Gefahren im Bereich Information Security hinzuweisen. Wir geben ihnen Tipps an die Hand, um Troy keine Angriffsfläche zu bieten und Risiken zu umgehen oder zu vermeiden.

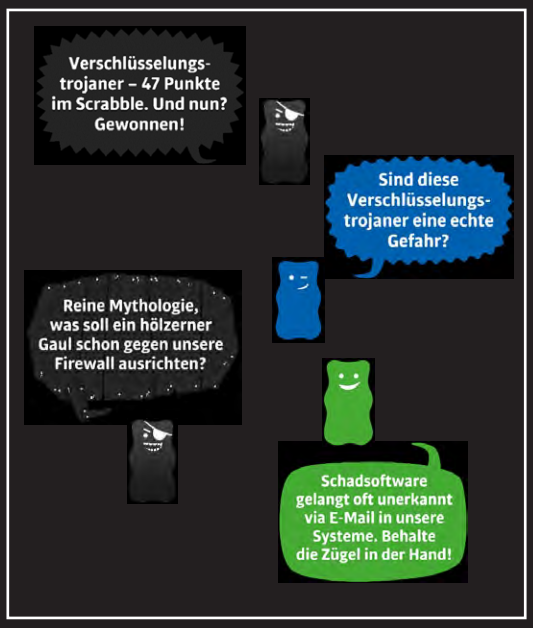
Mit unserem Claim, dem gezielten Einsatz von Troy und einer ganz direkten Kommunikation schaffen wir es, die Mitarbeitenden mit unseren Botschaften zu erreichen.«

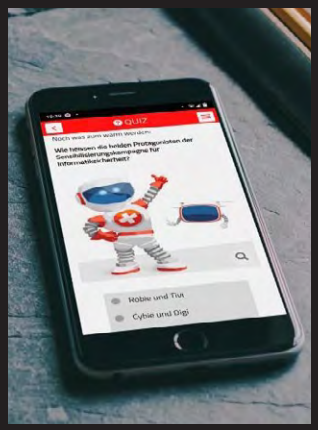
Care4Aware: Nominiert in der Kategorie PROMOTE:
IWC Schaffhausen
WATCH IT – der 360-Grad-Blick auf IT und Sicherheit bei IWC (2019 ff.)



»Die Wortmarke WATCH IT spielt offensichtlich mit dem englischen Aufruf zur Vorsicht, dem Kürzel für Informationstechnik (IT) und unserem Kernprodukt, der Uhr (Watch). Durch den Verzicht auf einen rein auf Informationssicherheit fokussierten Namen erschließen wir das Themenfeld der Digitalisierung und schaffen uns den Freiraum, künftig im Rahmen der Kampagne sämtliche aus unserer Sicht relevanten Themen zu behandeln. WATCH IT als Slogan signalisiert den Aufbruch in ein neues Zeitalter: das der Digitalisierung. Das visuelle Erscheinungsbild ist modern und klar. Layoutete Inhalte sind an moderne Magazingestaltung angelehnt, um die Lesbarkeit zu erhöhen und die Informationsvermittlung zu erleichtern.«

Care4Aware: Nominiert in der Kategorie PROMOTE:
Bundesamt für Informatik und Telekommunikation BIT: „Security Dialogue“ (2019 ff.)





»Unsere Sensibilisierungskampagne möchte die Mitarbeitenden nicht einfach nur dauerhaft mit Wissen zu Informationssicherheit berieseln, sondern aktiv mit ihnen in den Dialog gehen. Dialog bedeutet auch, verschiedene Sichtweisen und Blickwinkel zu berücksichtigen und kontrovers zu diskutieren.

Unsere IT-Bärlis stehen dafür Pate: sie symbolisieren diese verschiedenen Aspekte. Unser schwarzes Bärli ist der Bad Guy des Trios – immer unvorsichtig und ohne Rücksicht auf Verluste in der digitalen Welt unterwegs. Das grüne Bärli ist der pflichtbewusste Richtigmacher der Truppe, besonders vorsichtig und sensibilisiert. Und das blaue die Stimme der Informationssicherheit des BIT.

Damit es nicht langweilig wird, wandelt unser blaues Gummibärli sich farblich immer mal wieder. Denn unser Haus hat auch viele Farben und Facetten, und so soll das große Spektrum, die verschiedenen Stimmen und Sichtweisen der BIT-Anspruchsgruppen dargestellt werden.

Und warum jetzt Gummibärli? Das ist einfach: viele von euch kennen die große Gummibärli-Schale in der Abteilung IT-Sicherheit, die so gern besucht wird. Da lag es nahe, diese süßen Gesellen als kommunikative Botschafter zu nehmen für mehr Informationssicherheit beim BIT.

Die Sympathieträger sind zudem sehr redselig, untereinander, aber auch im Gespräch mit den Mitarbeitenden. Sie nehmen kein Blatt vor den Mund und sprechen Dinge unumwunden aus. Denn nur so können wir eine stabile Sicherheitskultur erreichen, wenn wir offen über Sicherheit reden. Das wünschen wir uns auch von den Mitarbeitenden.«

Care4Aware: Nominiert in der Kategorie PERFORM: Hochschule Luzern: „eBanking – aber sicher“ (2009 ff.)

»«eBanking – aber sicher!» ist eine Awareness-Kampagne in der Schweiz, die seit über 10 Jahren erfolgreich Mitarbeitende des Finanzsektors und die Schweizer Bevölkerung für sicheres E-Banking sensibilisiert. Gestartet im Jahr 2009 mit drei Pilot-Partnerbanken (Credit Suisse, PostFinance und Zürcher Kantonalbank), unterstützen die Kampagne heute knapp 50 Partnerbanken aus der ganzen Schweiz. Die Sensibilisierung baut mehrsprachig auf vier Grund-Pfeiler auf:

(1) Website: Damit die Endanwender ihren Computer und ihr Smartphone auf einen hohen Sicherheitsstand bringen und halten können, benötigen sie Unterstützung in Form von Regeln und Tipps. Diese Unterstützung hat auch zum Ziel, die Benutzer zu einem sicherheitsbewussten Verhalten während der E-Banking-Sitzung anzuleiten.

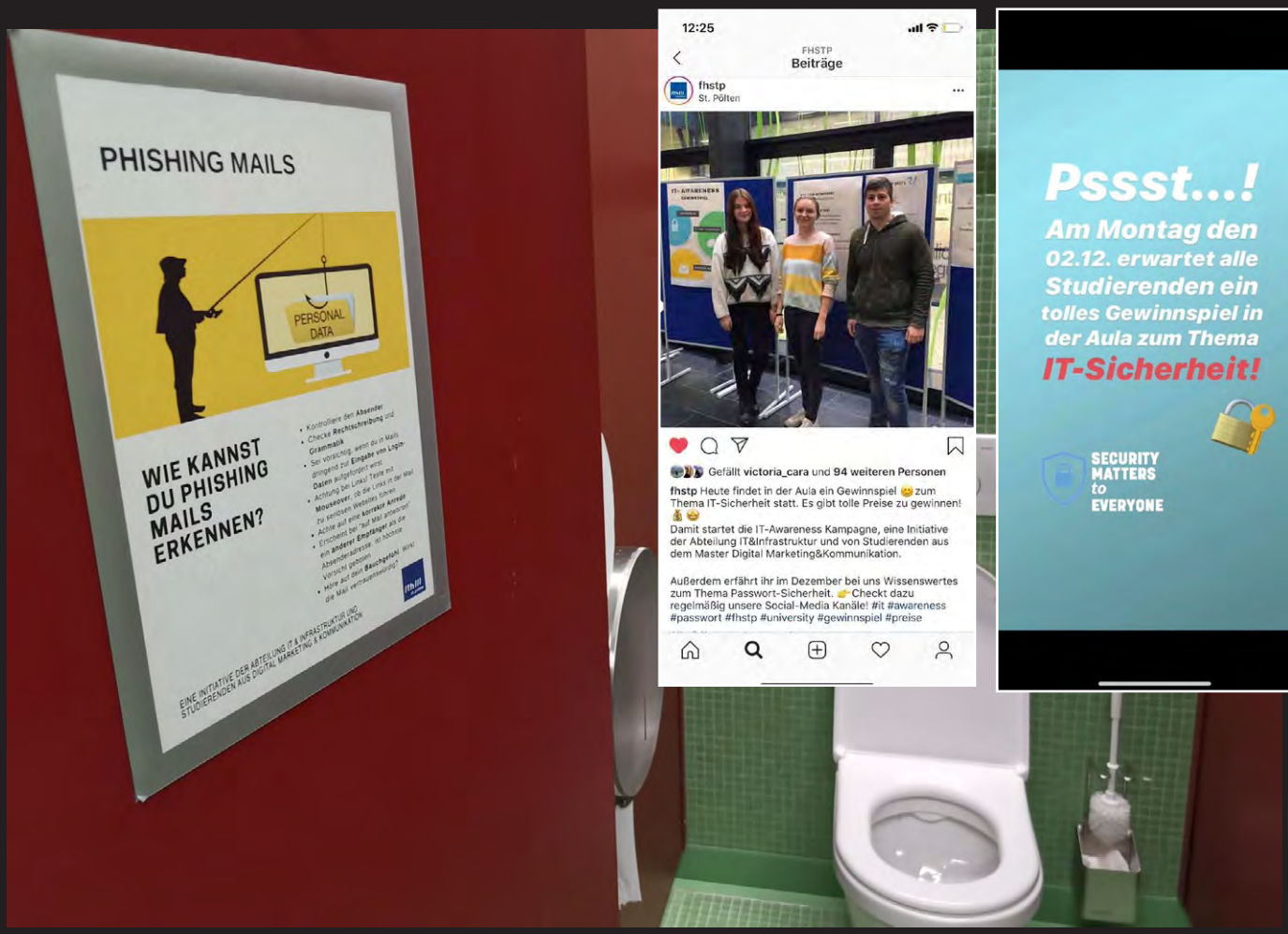
(2) Kurse für Endkunden: Leichtverständliche Kurse für Endkunden an verschiedenen Standorten in der ganzen Schweiz mit Informationen zu allgemeinen Computer-Sicherheitsfragen und insbesondere zur Sicherheit beim E-Banking.

(3) Medien-Monitoring: IT-Sicherheitsspezifisches Monitoring mit Fokus eCommerce und Endkunde der wichtigsten Medien; aktives Beobachten der Medienlandschaft und unmittelbares Erarbeiten und Verbreiten von ggf. notwendigen Stellungnahmen zuhanden der am Projekt beteiligten Finanzinstitute.

(4) Schulung der Kundendienstmitarbeitenden: Schulung der Endkundenberater und der Mitarbeitenden der Helpdesks, damit diese das Thema IT-Sicherheit kompetent abdecken können.

Die Website wird aktuell monatlich von knapp 40‘000 Besuchenden aufgerufen und über 1’200 Mitarbeitende der beteiligten Finanzinstitute sowie über 4‘800 Personen wurden bis heute in EBAS-Schulungen und -Kursen für sicheres E-Banking ausgebildet.«

Care4Aware: Nominiert in der Kategorie PERFORM: Fachhochschule St. Pölten GmbH (2019-2020)



Relevanz – zunehmende Phishingattacken an der Hochschule, z. T. Credential theft

Drei Hauptthemen – „Passwortsicherheit", „Schutz vor Phishing", „Sicherheit bei Cloudspeichern"

Interaktiv – Nutzung von Instagram-Stories und Gewinnspiel

Multichannel – gleichzeitige Verwendung von Online- wie auch Offline-Kanälen

Diversität – verschiedene Zielgruppen aus verschiedenen Fachgebieten (Studierende, MitarbeiterInnen, LektorInnen) mit verschiedenen Kanalnutzungen und diversem Wissen

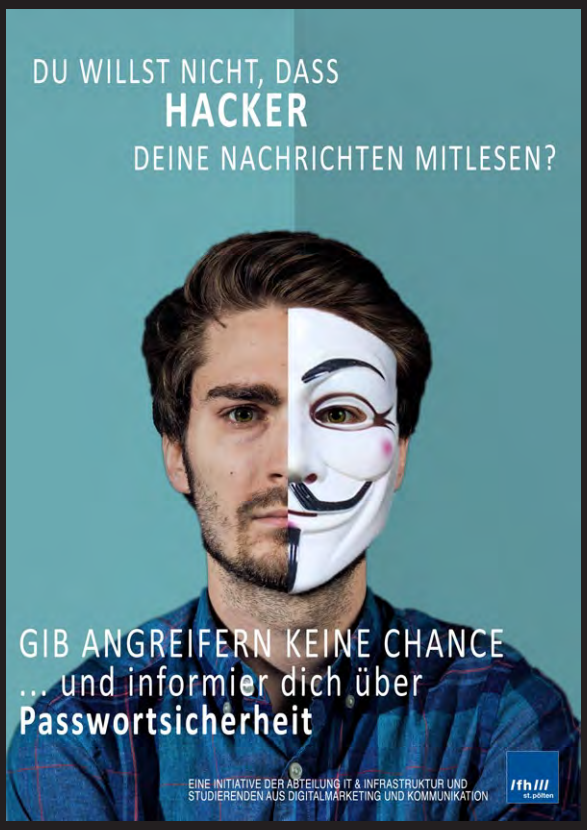
Ungewöhnliche Methoden – Plakate & Folder in der Mensa, Plakate in den Toiletten

Kick-off mit Gewinnspiel – aufmerksamkeitsstarker Auftakt mit Dialogmöglichkeit, Interesse geweckt

Projekt – von Studentinnen für Studierende konzipiert

Feedback – sehr positives Feedback auch von IT-Security-Studierenden wurde erhalten

Nachhaltigkeit – Durch Wahl von interaktiven Kanälen wurde das Interesse und auch der Dialog geweckt und eine Diskussion gestartet«



Care4Aware: Nominiert in der Kategorie PERFORM: Daimler AG: „Hacktoberfest“ (2019)

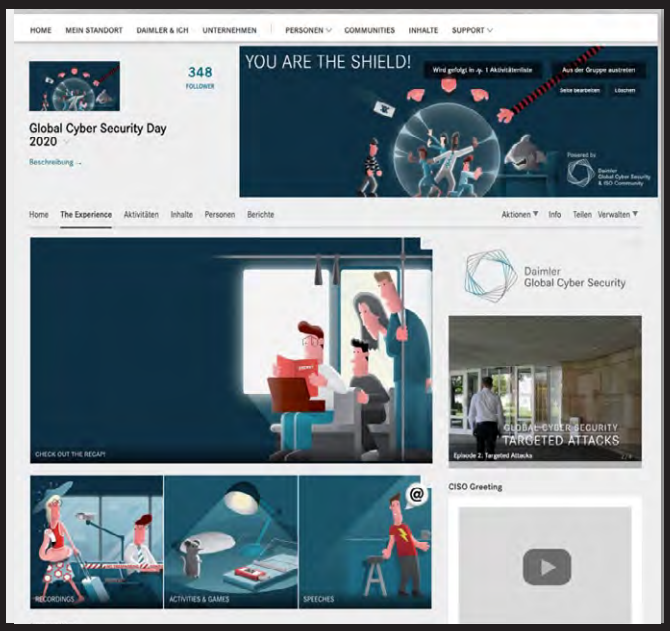
Impressionen der Kampagne

»*Die Kommunikation an die Mitarbeiter startete Anfang September mit der Mystery Challenge „Game of Codes“ im Social Intranet. Das onlinebasierte Kreuzworträtsel wurde mit einem Lösungsblatt kombiniert, welches sowohl am Computer oder in ausgedruckter Form genutzt werden konnte. Der Cyber Security Day unter dem Motto „Hacktoberfest“ wurde am 01. Oktober 2019 über den Unternehmenskanal angekündigt.*

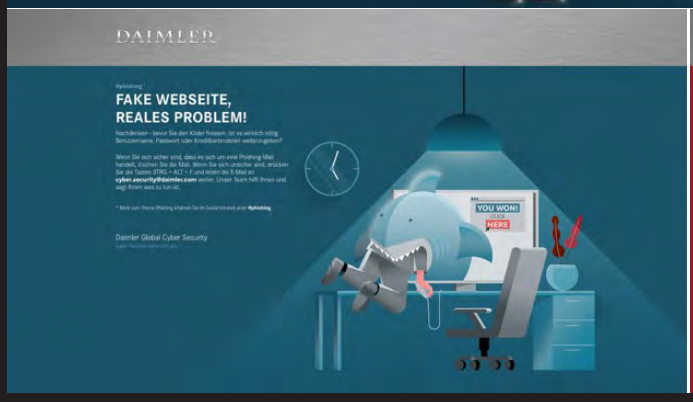
Ergänzend wurde eine eigene Social Intranet Community geöffnet, die nicht nur weitergehende Informationen zum Programm der einzelnen Standorte anbot, sondern auch intensiv für die Begleit- und Nachkommunikation der verschiedenen Länder genutzt wurde. In Summe haben 26 Länder an der Kampagne mit mehreren Standorten teilgenommen (alleine in Deutschland sind die zahlreichen verschiedenen Produktions- und Verwaltungsstandorte zu berücksichtigen).

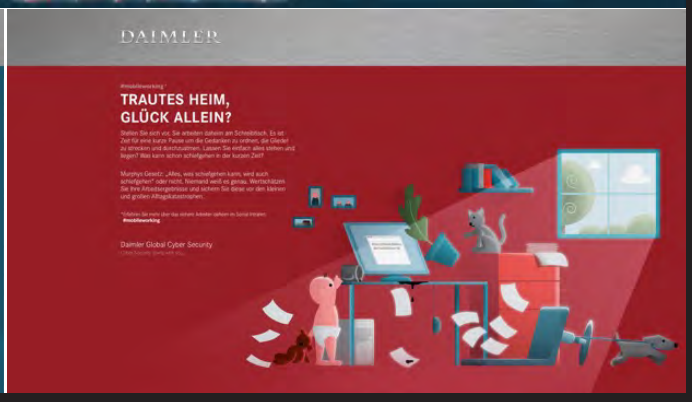
An Marktständen wurden definierte Cyber Security Themen und die damit verbundenen Risiken durch Aktivitäten, dem Einsatz von Gamification und durch den direkten Dialog vertieft und die Mitarbeiter sensibilisiert. Die Kampagne ist preiswürdig, da es eine Kampagne ist, die zwar zentral koordiniert wurde, jedoch dezentral von den lokalen Märkten für die Mitarbeiter umgesetzt wurde. Hierdurch konnten nicht nur kulturelle Besonderheiten berücksichtigt werden, sondern die lokale IT-Sicherheitsorganisation erreichte mehr Sichtbarkeit.

Die Verbindung von offline Aktivitäten mit der Online-Kommunikation ermöglichte ein Wir-Gefühl über die Standorte des Daimler-Konzerns und unterstützt die Kernbotschaften „Cyber Security beginnt mit Dir“ und „You are the Shield“.«

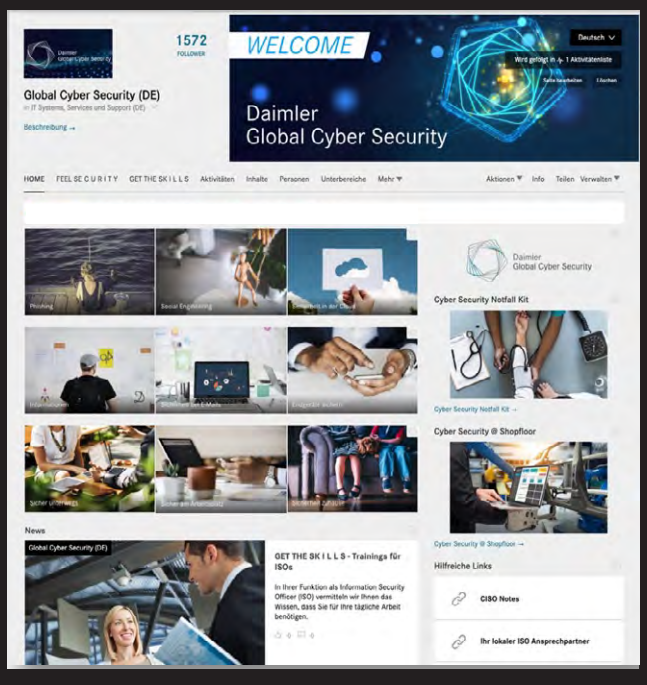


Care4Aware: Nominiert in der Kategorie CHANGE: Daimler AG: „Cyber Security beginnt mit dir“ (2018-2022)





» Das weltweite Cyber Security Awareness-Programm der Daimler AG orientiert sich an dem Claim „Cyber Security beginnt mit Dir!“ und hat zum Ziel Cyber Security im kollektiven Gedächtnis und mit einem gleichen Verständnis bei den Mitarbeitern zu verankern. Alle Aktivitäten rücken den Mitarbeiter und seinen Beitrag in den Mittelpunkt. Hierbei umfasst das Programm verschiedene Trainingsangebote je Zielgruppe (GET THE SKILLS), Kommunikation über verschiedene Kanäle (Online sowie Offline) als auch die Begleitung durch verschiedene Event-Formate (FEEL SECURITY) und Merchandising Artikel. Eine Messung des Wirkungsgrad des Programms erfolgt qualitativ anhand einer Mitarbeiterbefragung als auch quantitativ anhand von definierten Kennzahlen. Die Ganzheitlichkeit spiegelt sich nicht nur in der Gesamtverantwortung über die verschiedenen Mitarbeitergruppen (Mitarbeiter Verwaltung sowie Produktionsmitarbeiter) wieder, sondern auch in der Nutzung von verschiedenen, modernen Kommunikationskanälen und der qualitativen und quantitativen Erfolgsmessung. Diese ermöglicht eine konstante Überprüfung der Initiativen und unterstützt den flexiblen Ansatz auf Veränderungen zu reagieren.«



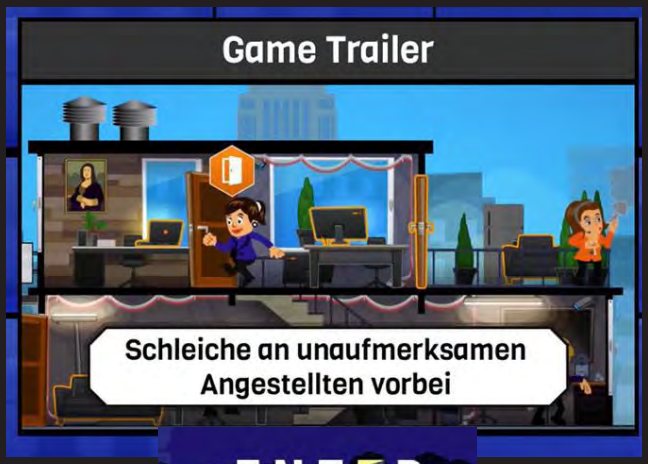
Care4Aware: Nominiert in der Kategorie CHANGE:
Stadt Zürich: „einfach sicher“ (2018 ff.)

»Die Organisation und Informatik (OIZ) setzt alles daran, Daten und Informationen im Verantwortungsbereich der Stadt Zürich mithilfe von zeitgemäßen organisatorischen und technischen Sicherheitsmassnahmen zu schützen. Aber: Keine noch so ausgeklügelte Technik bietet vollständigen Schutz, da bereits das Fehlverhalten einer einzelnen Person zu einem Verlust der Verfügbarkeit von städtischen Services oder zu ungewolltem Offenlegen von vertraulichen Daten führen kann. Umso wichtiger ist es, dass wir durch richtiges Verhalten alle zu einem sicheren digitalen Arbeitsumfeld beitragen.

Aus diesem Grund realisiert die OIZ in den Jahren 2018 bis 2020 (wieder) eine Sensibilisierungskampagne für Informationssicherheit. «einfach sicher» ist das Folgeprojekt der früheren Kampagnen «einfach SICHER 2.0» und «einfach SICHER», welche in den Jahren 2012 und 2007 in der Stadtverwaltung durchgeführt wurden.

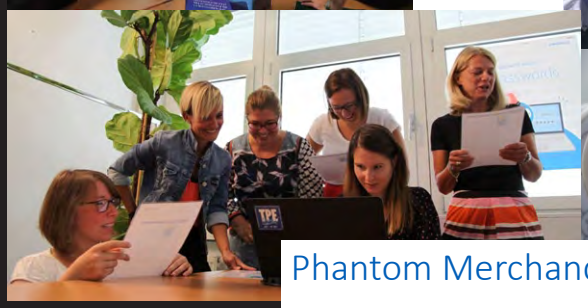
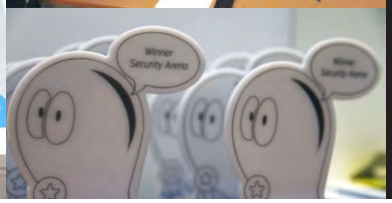
Über einen Zeitraum von 24 Monaten wird ein breites Portfolio von Aktivitäten angeboten, stets mit dem Ziel die Mitarbeitenden zu befähigen und einen Mehrwert zu erzeugen. Es werden die persönlichen Vorteile von sicherheitskonformem Handeln aufgezeigt, auch für das Privatleben. Und dabei geht es darum, die Mitarbeitenden nicht als inhärentes Risiko zu brandmarken, sondern stark zu machen – für die Herausforderungen der Digitalisierung.

In «einfach SICHER» bilden die größten (Verhaltens-) Risiken wie Phishing, Malware, Social Media die Themenschwerpunkte quer über die ganze Vielfalt der Stadt Zürich. So vielfältig wie die Arbeitsbereiche der Stadt sind, von der klassischen Verwaltung über Spitäler, industriellen Betrieben bis hin zu Blaulichtorganisationen so vielfältig sind auch die Aktivitäten: Online genauso wie mit physischer Präsenz, Videos, Newsletter aber auch ein Mini-Buch zum Angreifen und Mitnehmen. Live-Hacking-Shows, ein Security Parcours oder Workshops zum Thema „sicherer PC“ als kollektives Erlebnis ebenso wie ein Security Adventkalender oder ein Security Game für das individuelle Erfahren von Informationssicherheit. «



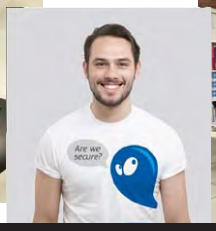
Care4Aware: Nominiert in der Kategorie CHANGE: Amadeus: „It's up to you“ (2014 ff.)



Phantom Merchandise




» Das Security Awareness-Programm von Amadeus läuft seit der Einsetzung des ersten CISO im Jahr 2014. Seitdem haben wir kontinuierlich durch verschiedene Trainingsmaßnahmen, Kommunikation und flächendeckendes Marketing den Awareness-Level unserer Mitarbeiter verbessert. Von Anfang an haben wir durch Überzeugungsarbeit beim Top-Management für breite Unterstützung unseres Programms gesorgt.

Sehr unterhaltsame On-site Trainings wie unser „Fit for Cyber Security“ mit Live-Hacking-Demos, unser “Security @Home” Training zum Schutz der Privatsphäre und die allseits beliebte Security Arena, ein Team Event mit Security Spielen, tragen dazu bei, eine positive Einstellung zum Thema Security zu entwickeln und das eigene Verhalten schrittweise zu verbessern.

Darüber hinaus veranstalten wir spezielle Trainings für Manager, System Engineers und für Software Entwickler. Um wirklich alle unserer 21.000 Mitarbeiter an 150 Standorten weltweit zu erreichen nutzen wir ein modular aufgebautes E-Learning, das wir in Englisch, Deutsch, Französisch und Spanisch eingesprochen und untertitelt haben. Seit 2019 haben wir auch eine spezielle Version für Menschen mit Sehbehinderung.

In Zusammenarbeit mit unserer Corporate Communications Abteilung kommunizieren wir schwerpunktmäßig drei- bis viermal im Jahr spezielle Themen über alle uns zur Verfügung stehenden Kanäle: Amadeus Intranet Homepage, Leadership Blogs, Artikel im Weekly Newsletter, TV-Spots, Videos, Poster etc. Unsere eigene Security & Privacy Community im Intranet enthält alle relevanten Informationen zum Thema Informationssicherheit an einer Stelle.

Seit 2016 hilft unser Maskottchen, das Friendly Phantom, bei der Verbreitung unserer Botschaften. Diese bei unseren Mitarbeitern sehr beliebte Figur wird auf Promotionmaterialien und auf sämtlichen Marketingmaterialien zum Thema Informationssicherheit im ganzen Unternehmen sichtbar verteilt. Das positive Image des Phantoms überträgt sich auch auf die Mitarbeiter und die Arbeit der Sicherheitsabteilungen.

Wir messen den Erfolg über quantitative Indikatoren wie die E-Learning Abschlussquote, die Fehlerquote bei Phishing, die Anzahl der gemeldeten simulierten und echten Phishing E-Mails, sowie die Anzahl gemeldeter Sicherheitsvorfälle. Zusätzlich haben wir die Resultate der Awareness-Umfragen 2016 und 2018 und qualitative Indikatoren wie z. B. die hohen Anmelderaten bei freiwilligen Trainings und das positive Feedback von Management und Belegschaft.«

MBSR = MINDFULNESS BASED SECURE REACTION?

WAS HAT MBSR MIT SECURITY AWARENESS ZU TUN?

VON ANKHA HAUCKE & DIETMAR POKOYSKI

Als wir mit known_sense 2004 nach dem vermeintlichen Zufallserfolg infolge der Biertischidee eines Virusquartetts als Sensibilisierungs-Tool erstmals in Kontakt mit dem Bereich Security Awareness kamen, erschloss sich für uns ein Feld, in dem methodisch vor allem die Lerntheorie heraus stach. Das heißt der Mitarbeiter mehr oder weniger als lebender Kassettenrekorder, dem man mit Regeln per Oldschool-Schulfernsehen impfte in der vagen Hoffnung, über die kognitiv-rationale Ansprache Compliance herzustellen. Dass eine derartige, rein sachliche „Schöner-Wohnen"-Formel nicht das Ende, sondern allenfalls der Anfang einer Awareness Next Generation sein könnte, lag bereits in der Luft, denn gerade im deutschsprachigen Bereich vertraten außer uns unter anderem Michael Helisch von HECOM Security Awareness Consulting oder Marcus Beyer (ex-DXC Technology) ebenfalls die Ansicht, dass Security Awareness nicht ausschließlich über klassische Didaktik oder – später – reine Simulation (wie u. a. bei Phishing-Tools) funktionieren kann, sondern Lernen bzw. „plattes" Training lediglich ein paar Prozentchen hierzu beitragen würden.

Vielmehr wurde nicht zuletzt über unsere psychologischen Wirkungsanalysen von Kampagnen deutlich, dass emotionale Faktoren (etwa unter Einbindung von Marketing & Co.) sowie systemische Kommunikation, d.h. der Kontakt mit sich selbst und seiner Umgebung (z. B. via Gamification) die eigentlichen „Awareness-Stars" und wahren Trigger nachhaltiger Sensibilisierung sind. Wir nennen dies das Prinzip „Talking Security", also das Reden über Sicherheit, fachlich gesprochen diskursive Settings zu schaffen, die die Zielgruppe in einen regelmäßigen Austausch zum Thema Informationssicherheit bringt.

Heute, mehr als 15 Jahre später, fragen wir uns, ob das Reden miteinander ausreicht, ob Content-getriebene Awareness-Maßnahmen – auch wenn Sie typische Marketing-Settings oder systemische Faktoren berücksichtigen – sich nicht grundsätzlich zu sehr beschränken auf etwas konstruiert Erwünschtes, eben Compliance herzustellen und den Mitarbeitern eine (statische) Anleitung bereit zu stellen, anstatt Kontakt (mit anderen, aber auch mit sich selber) zu fördern. Vielleicht müssen wir aufhören, die (kulturellen) Phänomene, die uns im Rahmen unserer Arbeit begegnen, zu „zerreden", zu überlagern. Gerade Sicherheitskultur umfasst noch mehr paradoxe Faktoren als die komplette Unternehmenskultur, die sich – gerade wegen der paradoxen Verhältnisse – stets einen Weg durch die Organisation bahnt, der oftmals weit entfernt ist von den erwünschten Ausprägungen sogenannter Corporate Identity. „Ent-Sicherungen", also Mitarbeiter-Fehler, sind in der Regel so „gemacht" wie auch Compliance (als Regelwerk) „gemacht" ist. Und aus unserer tiefenpsychologischen Social-Engineering-Studie „Bluff me if you can" wissen wir, dass es vielen Menschen schwer fällt, ihre eigenen Schwächen (bei sich) zu entdecken und zu benennen. Hier ist also der Social Engineer oft „schlauer" als man selbst. Das heißt: Ganz schön blöd, wenn ich (z. B. im Kontext von Social Engineering) die sozialen Stärken und Schwächen von Fremden bzw. ihre Motive, mit mir Kontakt aufzunehmen, beurteilen soll, das aber noch nicht einmal bei mir selbst schaffe.

Daran anknüpfend und weil wir in inzwischen beinahe 17 Jahren Awareness-Arbeit gelernt haben, dass rein-formale Compliance-Inhalte immer weniger wichtig sind im Defense-Kontext, plädieren wir für ein radikales Umdenken hinsichtlich der Instrumentarien bei Security Awareness-Kampagnen. Vergleichbar mit Webseiten schauen wir stärker auf die Trennung von Form und Inhalt bei zeitgleichem Verschmelzen von Arbeitsverfassung und deren Steuerung – unabhängig vom Faktor Sicherheit. Hierfür, d. h. hinsichtlich des Bewusstmachens meines Wirkens als Arbeitnehmer, existieren zahlreiche, auch in Organisationen erprobte Methoden, um die Aufmerksamkeit auf eine sichere Arbeitsumgebung zu lenken, z. B. Achtsamkeit bzw. MBSR (Mindfulness Based Stress Reduction, kurz auch Mindfulness genannt).

Was ist Achtsamkeit bzw. Mindfulness eigentlich?

Erstaunt schauen wir auf Unternehmen wie SAP (s. Kasten 1) mit seinem Corporate Mindfulness-Programm oder auf den französischen Fußballverband (s. Kasten 2), der Achtsamkeit in die Trainingsprogramme der Jugendnationalmannschaften integriert hat – mit etlichen Weltmeister-Teams. Achtsam zu sein bedeutet, sich des gegenwärtigen Augenblicks gewahr zu sein, ohne zu bewerten. Eine nichturteilende Wahrnehmung der Gegenwart geht mit einem umfassenden Bewusstsein einher, indem eben nicht von vornherein bestimmte Aspekte als wichtig und andere Aspekte als unwichtig bewertet und demzufolge z. T. nicht beachtet werden. Vielmehr werden alle Wahrnehmungen oder Eindrücke zur Kenntnis genommen, ohne dass man darauf reagiert. Im Vergleich zur gewohnten Alltagsverfassung geht eine achtsame Haltung insofern auch mit einer Entschleunigung einher, die einen Raum zwischen Reiz und Reaktion schafft. In diesem Raum ist es möglich, mit Bedacht und Weitblick eine „weise" Entscheidung darüber zu treffen, wie man weiter vorgehen will.

Achtsamkeitsübungen wie Sitzmeditation oder der Bodyscan haben nichts Esoterisches an sich. Sie dienen sehr pragmatisch dazu, zu üben, die Realität möglichst umfassend wahrzunehmen und zu akzeptieren.

Was wir in MBSR-Trainings lernen

MBSR ist ein auf buddhistischen Lehren fußendes Geistestraining. Es geht darum, den eigenen Geist besser kennenzulernen, zu verstehen, wie er funktioniert und die eigenen Geisteszustände aktiv zu beeinflussen anstatt permanent durch das Hamsterrad zu sausen. Dabei erlangen wir eine zunehmende Bewusstheit für bisher unbewusste Motive und damit einen größeren Entscheidungsspielraum, wie wir auf Herausforderungen reagieren wollen, z. B. ob wir eine E-Mail als Phishingmail identifizieren oder eben nicht. Wir können lernen, aus Reaktionsmustern auszusteigen, die sich bisher als zwangsläufig angefühlt haben, häufig aber nicht zielführend sind. Wir können sozusagen aus dem „Autopiloten" aussteigen und uns für (z. B. sichere) Verhaltensweisen entscheiden, die auf einem Weitblick beruhen, die viele Aspekte der gegebenen Situation einbeziehen statt nur die momentan vordergründigen, bezogen auf Informationssicherheit etwa wichtige Details meines Handelns, z. B. Detektion von Risiken einer eingehenden E-Mail statt flüssigen Durchkommens in Bezug auf mittel- und langfristige Arbeitsziele (die zwar ebenfalls wichtig sind, aber gegebenenfalls Sicherheitsrisiken verstärken).

Hirnphysiologisch betrachtet kann man stark vereinfacht sagen, dass wir dazu neigen, in Stress-Situationen stark automatisierte Reaktionsmuster abzurufen, die in früheren Phasen der Menschheitsgeschichte sinnvoll waren und dem so genannten Reptiliengehirn zugeordnet werden. Dabei sind wir in einer Verfassung, die mit einem Tunnelblick verbunden ist, der sich auf wenige Aspekte der gegebenen Situation fokussiert. Für unsere Vorfahren war das sicher eine sinnvolle Überlebensstrategie. Heute jedoch befinden wir uns selten in unmittelbarer Lebensgefahr. Bedrohliche Entwicklungen sind schwerer zu erfassen und erfordern das Verfolgen langfristiger Ziele, ein Durchdenken komplexer Zusammenhänge. Wir können üben, automatisierte Reaktionsmuster zu ersetzen durch Verhaltensweisen, die der Komplexität unserer modernen Welt gerecht werden und vom Neocortex gesteuert werden. Der Neocortex ist der evolutionsgeschichtlich jüngste Teil des Gehirns, mit dessen Hilfe wir auch abstrakte Zusammenhänge erfassen und verschiedene Teile des Gehirns koordinieren können.

Die Psychologie von Incidents

Wenn wir Sicherheitsmaßnahmen nicht konsequent einhalten, sind wir „unachtsam", d. h. unser Verhalten wird in diesem Moment von Motiven bestimmt, die nicht unseren langfristigen Zielen dienlich sind (s. a. „Ich bin der Fehler – Schuld, Scham, Viktimisierung bei Social Engineering" in der Erstausgabe unseres Magazins). Im Autopilotenmodus ist unsere Wahrnehmung auf vordergründige Aspekte der Situation beschränkt. So etwa im Kontext Social Engineering, z. B. dass ein mir fremder Mensch mich freundlich um eine (vertrauliche) Information bittet und ich es gewohnt bin, (automatisch) behilflich sein zu wollen. Das Helfen ist für viele Menschen die am besten eingeübte und am leichtesten abrufbare Reaktion, wenn sie um etwas gebeten werden. Sich in einer solchen Situation bewusst zu machen, dass die Freundlichkeit des Fremden unecht, seine Bitte unberechtigt sein und die Erfüllung seiner Bitte negative Konsequenzen in der Zukunft haben könnte, erfordert ein Gewahrsein für subtile und z. T. nicht unmittelbar wahrnehmbare Aspekte der Situation. Dazu kann das berühmte „Bauchgefühl" (Intuition) gehören, was man verstehen kann als eine körperliche Reaktion auf eine Beunruhigung oder subtile Sorge im Kontext non- oder paraverbaler Kommunikation. Je achtsamer ich eine solche Reaktion wahr- und ernstnehme, desto konstruktiver kann ich sie in meine Entscheidungsfindung einbeziehen. Es kann aber auch von entscheidender Bedeutung sein,

Beispiel 1: SAP

SAP hat mithilfe des Wirtschaftsingenieurs, Coach, Trainers und Directors von SAP Global Mindfulness Practice, Peter Bostelmann, Achtsamkeitskurse bereits 2013 eingeführt und ein globales Programm daraus entwickelt. Bostelmanns Team hat sich zum Ziel gesetzt, Achtsamkeitspraktiken zur Verbesserung von Führung, Produktivität und Wohlbefinden unter den Mitarbeiterinnen und Mitarbeitern zu kultivieren. In diesem Kontext bietet das Unternehmen das zweitägige Achtsamkeitsseminar „Search Inside Yourself" (SIY) an, das ausschließlich von eigenen Personal betreut wird. 43 SAP-Mitarbeiter haben hierfür eine Trainerausbildung absolviert und insgesamt 7.000 Kollegen und Kolleginnen an insgesamt 48 Standorten im Rahmen eines SIY-Kurs angeleitet. Neben den Seminaren gibt es weltweit vielfältige Vertiefungsangebote, wie achtsame Mittagessen, Achtsamkeitsnachmittage oder virtuelle Sessions.

Bostelmann spricht von einem 200-prozentigen Return on Investment, der sich neben den Umfragewerten der Teilnehmer auch anhand des gestiegenen Employee Engagement Index und des Rückgangs an Krankheitsausfällen messen lässt. Diese Werte wirken sich auch auf das Geschäftsergebnis aus. Der Betriebsgewinn von SAP steige um 50 bis 60 Millionen Euro pro Anstieg des Employee Engagement Index um einen Prozentpunkt. Ein Prozentpunkt mehr beim Business Health Culture Index (dieser Wert sowie der Employee Engagement Index werden bei der jährlichen People Survey gemessen) bedeute sogar 85 bis 95 Millionen Euro mehr Gewinn.

Von diesem Erfolg profitieren inzwischen auch die Kunden und Partner der SAP. Wie es dazu kommt, beschreibt Bostelmann: „Auch andere Unternehmen sehen, wie die Reizüberflutung in Zeiten der Digitalisierung immer größer wird." Dass die SAP ihr Achtsamkeitsprogramm erfolgreich ausbaut, stößt inzwischen unter externen Medien auf große Resonanz. „Viele Kunden wie Siemens und Deutsche Telekom möchten von unserem Best-Practice-Modell lernen," sagt Bostelmann. Daher entsendet SAP die eigenen Achtsamkeitstrainer. Sie gehen als strategische Berater zu Kunden, um diesen zu helfen, in deren Organisation Achtsamkeitsangebote für Mitarbeiter zu schaffen. Sie geben dort direkt SIY-Seminare, oder bilden sogar Trainer beim Kunden aus. Bostelmann findet: „Für die SAP ist das eine Chance, Kundenbindungen zu verstärken. Zugleich geht das Unternehmen mit gutem Beispiel voran und leistet einen gesellschaftlichen Beitrag, der in die Unternehmensvision ‚Help the World Run better and improve people's lives' einzahlt." *(Quelle: https://news.sap.com/germany/2018/09/achtsamkeit/)*

mögliche langfristige Folgen meines Verhaltens zu bedenken und in ein Verhältnis zu setzen zu dem unmittelbareren Bedürfnis, freundlich sein, wie z. B. eine potenzielle Rufschädigung des Arbeitgebers.

MBSR = Mindfulness Based Secure Reaction?

Führt MBSR unweigerlich zu „Mindfulness Based Secure Reactions"? Nicht unbedingt. Wenn wir lernen, einen Puffer zwischen Reiz und Reaktion zu bringen, bedeutet das, dass wir die Realität umfassender wahrnehmen, wozu auch unsere eigenen Impulse bzw. Motive gehören. Mit zunehmender Achtsamkeit nehmen wir auch Impulse wahr, die wir in der üblichen Alltagsverfassung meistens verdrängen. So können wir bewusster entscheiden, wie wir reagieren wollen. Unbewusste und unbedachte Reaktionen, die wir im Nachhinein bereuen, nehmen damit ab. Theoretisch können wir uns allerdings auch bewusst dagegen entscheiden, uns den Sicherheitsbestimmungen bzw. Policies gemäß zu verhalten. Wenn ein Arbeitnehmer sich bei seiner Arbeit nicht wohl fühlt wird er nach einer Achtsamkeitsschulung vielleicht deutlicher als zuvor wahrnehmen, dass er im Falle eines vermuteten Incidents Genugtuung bei der Vorstellung empfindet, sich nicht sicherheitskonform zu verhalten und der Firma damit zu schaden. Er wird dann aber wahrscheinlich auch gegenläufige Tendenzen wahrnehmen wie z. B. Angst vor Konsequenzen und Skrupel. Es lässt sich inzwischen wissenschaftlich belegen, dass Achtsamkeitstrainings Dankbarkeit und Mitgefühl fördern. In einer achtsamen Verfassung werden also die allermeisten Menschen neben einer potenziellen Versuchung auch Skrupel empfinden.

Unspezifischer Zusatznutzen von MBSR

Meditation ist eine – zumindest für westliche Hirne – paradoxe Sache. Wir können sie nicht wie eine Medizin anwenden, um eine bestimmte Wirkung anzustreben bzw. „Heilung" zu erzielen. Und sie kann eben auch nicht verordnet werden wie etwa eine medizinische Behandlung. Vielmehr geht es in Meditation darum, absichtslos und ohne Wertung wahrzunehmen, was ist, ohne irgendetwas verändern zu wollen. Zugleich wissen wir dabei um den Effekt der zunehmenden Klarheit des Geistes mit den Begleiterscheinungen der Verringerung von Leid, der zunehmenden Freiheit, Dankbarkeit und Freude. Dieser logische Widerspruch kann nicht wirklich erklärt, sondern muss erfahren werden. Allerdings stellt sich die Erfahrung von zunehmender Gelassenheit recht schnell ein, wenn wir in Stille sitzen und uns z. B. auf die Atemempfindungen fokussieren. Dabei wird letztlich geübt, sich aktiv von Gedanken und Gefühlen zu distanzieren, statt sich davon überwältigt oder vereinnahmt zu fühlen. Insofern ist Meditation alles andere als Nichtstun, sondern harte Arbeit.

Aktuell existieren noch keine seriösen Studien darüber, ob Achtsamkeit bzw. MBSR produktiv auf eine sichere

Beispiel 2: Französischer Fußballverband FFF

Der französische Fußballverband Fédération Française de Footbal war weltweit der erste Sportverband, der „Bewusstheit" und „Selbsterkenntnis" in sein Ausbildungsprogramm für Jugendnationalmannschaften integriert hat – mit großen Erfolgen wie die große Titelsammlung belegt. Über diese Initiative existiert auch ein Dokumentarfilm von Anja Krug-Metzinger „Das stille Leuchten", über das das TAKE AWARE sec&life magazine in der Ausgabe 1 bereits berichtete. Der Film zeigt, welche Erfahrungen Kinder und Jugendliche mit Trainingsmethoden machen, die die klassische Achtsamkeitsmeditation, soziale Selbsterfahrung und Körperbewusstsein mit der Schulung einer globalen Perspektive und kritischem Engagement verbinden. *(Quelle: http://www.krug-metzinger.de/docs/Silles-Leuchten.pdf)*

Umgebung bzw. mehr Defense im Kontext Informationssicherheit einzahlt. Ausgehend von unseren Beobachtungen und den positiven Erfahrungen bei Unternehmen wie SAP et al. (s. Kasten 1 bzw. 2) ist jedoch davon auszugehen, dass Kollateraleffekte wie das generelle Wohlbefinden der Mitarbeiterinnen und Mitarbeiter an ihrem Arbeitsplatz sowie Konzentration, Mitgefühl, Empathie und Persönlichkeitsentwicklung zu einer Entschleunigung im Umgang mit Informationssicherheitsrisiken führen und damit auch die Security Awareness (zumindest implizit) steigern.

PHISHING SIMULATIONEN – SEXY SECURITY ODER PHISHERS FRITZ?

ELEVATOR PITCH PHISHING

KOMPILIERT VON MARCUS BEYER
EINLEITUNG VON DIETMAR POKOYSKI

Eine Phishing-Simulation ist per se weder ein Planspiel bzw. generell gamifiziertes Tool, noch ein Awareness-Instrument, sondern eine Testumgebung, bei der das Verhalten von Mitarbeitern in Bezug auf den Umgang mit E-Mails überprüft und mithilfe eines quantitativen Ansatzes in Kennzahlen überführt wird. Eine Security Awareness-Maßnahme wird erst dann daraus, wenn die Simulation einer didaktischen Dramaturgie folgt und lerntheoretische Benefits umfasst (bedient Awareness-Layer 1: Wissen bzw. -Layer 3: Können) oder die Simulation selbst bzw. die Ergebnisse der damit verknüpften Evaluation Anlässe für verknüpfte Kommunikationsmaßnahmen bilden (bedient Awareness-Layer 2: Wollen).

Synergetische Maßnahmen beachten

Verknüpfte Kommunikations-Maßnahmen, die eine Phishing-Simulation aufladen und damit sexier gestalten, können unter anderem sein:

- Informelle oder visuelle Kommunikation der kompletten Simulation oder der Ergebnisse, z. B. Reports, FAQs, Glossar, Artikel im Intranet oder Mitarbeitermagazin, Text- und/oder Beiträge in internen Social Media-Plattformen, Lernkarten und/oder Plakate, Aufsteller, Anzeigen & Co., die die Ergebnisse visualisieren
- Diskursive Formate, um Ablauf, Erfolg und/oder Ergebnisse zu thematisieren, z. B. Workshops, Team-Meetings, Video-Konferenzen, Social Media-Plattformen u. ä.
- Incentivierung der Simulation bzw. ihrer Ergebnisse nach Erhöhung der gamifizierten Anteile
- Synergetische Maßnahmen zum Thema Phishing oder assoziierter Themen, z. B. Social Engineering, Desinformation etc., etwa Präsenztrainings, gamifizierte Instrumente, Live-Kommunikation, Virales, Flurfunk, Mitarbeiter-Wettbewerbe, Videos, Animationen, Key Visuals, Giveaways, um das Thema als Ganzheit darzustellen und ggf. diverse Lerntypen, Zielgruppen und psychologische Verfassungen zu bedienen

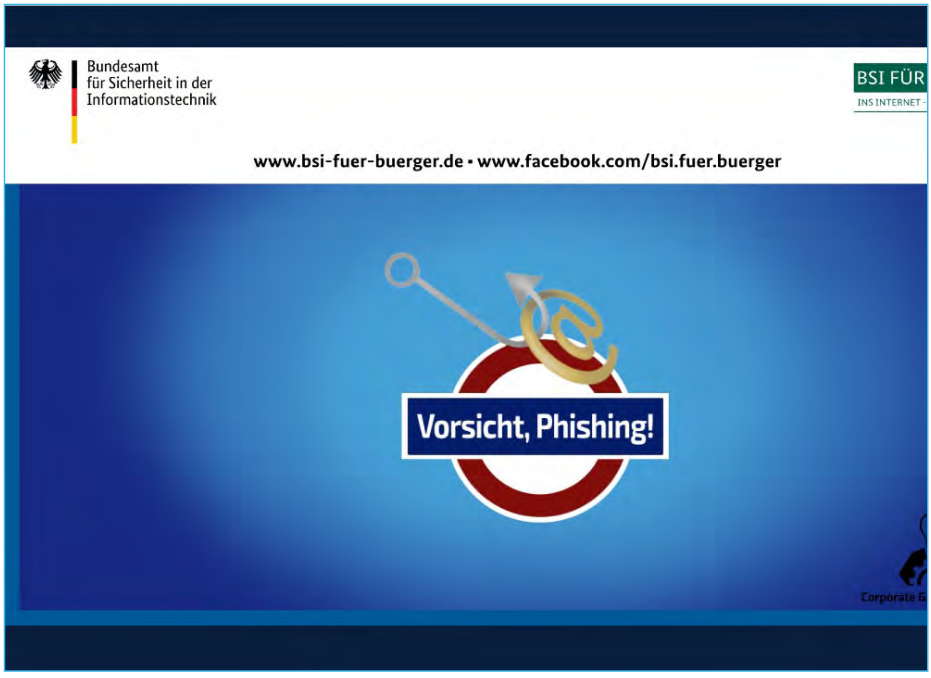
Den Anwendern von Phishing-Simulationen ist bewusst, dass dem Format ein gewisses Maß an Finger-Pointing inhärent ist, das im Worst Case das Risiko eines Desavouierens in Kauf nimmt. Daher ist die Reduktion von potenzieller Reaktanz bei den Mitarbeitern einer der wichtigsten Aspekte bei der Implementierung von Phishing-Simulationen. Je nach unternehmens- bzw. sicherheitskulturellen Bedingungen sind daher der Zeitpunkt der Einbettung in eine übergeordnete Maßnahme bzw. Kampagne, Wording und Ansprache und Auswahl bzw. Intensität von begleitenden Kommunikationsmaßnahmen zu beachten.

Immer nur so gut wie das Konzept

Im Zweifelsfall lohnt sich der Wechsel auf rein spielbasierte Lösungen mit dem geschützten Rahmen eines Game-Frameworks außerhalb des eigenen E-Mail-Clients. Die Firma mybreev bietet mit dem Digital-Spiel „Phished again“ eine Alternative zu herkömmlichen Phishing-Simulationen, die ebenfalls in Bezug auf das Verhalten im Umgang mit E-Mails trainiert, auf das hier explizit hingewiesen sei, weil es nicht im Pitch auf den folgenden Seiten behandelt wird.

Fazit: Awareness-Maßnahmen innerhalb von umfangreichen Security Awareness Change-Kampagnen greifen immer häufiger auf Phishing-Simulationen zurück. Diese müssen aber im Sinne integrierter Kommunikation „schlau“ ins Gesamtkonzept eingebunden sein, um eine nachhaltige Wirkung erzielen und proaktiv hinsichtlich möglicher Widerstände agieren zu können Am Ende kommt es also auf ein treffendes Gesamt-Konzept bzw. das Security Awareness-Framework an, um eine Phishing-Simulation erfolgreich zu gestalten.

Wir bedanken uns bei allen Teilnehmern für ihre freundliche Mitarbeit an diesem qualitativen Benchmark und insbesondere Marcus Beyer für seinen Input und die geduldige Steuerung.



„Phished again“ in der BSI-Version

ELEVATOR PITCH PHISHING (1/2)

Tool/Anbieter	HoxHunt	IT-Seal
	HOXHUNT	IT-SEAL Social Engineering Analysis Labs
Referent	Juha Heikkila und Thomas Schlienger (Treesolution)	David Kelm Geschäftsführer
Frage 1: Warum ist eine Phishing-Simulation aus Ihrer Sicht ein geeignetes Instrument innerhalb von Sensibilisierung-maßnahmen?	People can be aware of the threats but still fall into attacks as we have seen. The reason is that social engineering is aimed to attack and provoke emotions in the recipient and based on different studies in human behavior it is almost impossible to teach a person that "if you feel fear then you need to do x, y and z". This factor is usually the reason traditional e-learning and manual phishing tools have not been able to deliver the desired results for the security awareness programs. Therefore, the employees need to be trained in behavior rather than "awareness".	Gefährdendes Verhalten geschieht häufig durch das von Daniel Kahnemann beschriebene "schnelle Denken"(unüberlegte Reaktionen oder „langsame Denken" – also durch „automatisierte" Verhaltensweisen). Um Automatismen zu beeinflussen, ist es bedingt hilfreich, wenn Sensibilisierung das „langsame Denken" beeinflusst (z. B. E-Learning, Präsenzschulungen). Für eine effektive Veränderung des „schnellen Denkens" ist sofortiges Feedback an den Nutzer essentiell – z. B. über Phishing-Simulationen. Der Klick auf einen Phishing-Link setzt den „Most Teachable Moment" mit Erklärungen für den Nutzer frei. Durch dieses Erfahrungslernen lässt sich das Verhalten nachweisbar verbessern, während einmalige Maßnahmen nur kurzfristige Effekte zeigen. Gleichzeitig bieten Simulationen die Möglichkeit, den Lernerfolg zu überprüfen und zielgruppenspezifische Maßnahmen zu nutzen.
Frage 2: Welche Rolle spielen Assesments/KPIs aus Ihrer Sicht für den Erfolg von Sensibilisierungs- und Schulungsmaßnahmen?	At Hoxhunt we believe that success is much more important than failure. The main measurement is activation and engagement levels within the employees. The old-world main measurement has been failure percentage. That might lead frustration and distracting behavior among the employees, when they feel that information security team is testing them. With Hoxhunt approach, we start with easy enough training that every employee is able to have successful moments and then make the training gradually more harder by increased skillset.	Eines der bislang größten Probleme in der IT-Sicherheit ist, dass man kaum messen kann, wie sicher man eigentlich ist und was eine bestimmte Investition an Sicherheitsgewinn gebracht hat bzw. bringen wird. Dies führt vor allem dazu, dass das Management häufig Investitionen in die IT-Sicherheit kritisch gegenüber steht. Um dieses Dilemma zu überwinden, ist es unverzichtbar, Kennzahlen in der IT-Sicherheit einzuführen. Darüber hinaus helfen solche Erfolgsmessungen zu entscheiden, wie die Awareness für die einzelnen Gruppen weiter (bis zum gewünschten Ziel-Niveau) gesteigert werden kann.

Lucy/ Clue Security Service	Proofpoint/Wombat	SoSafe
SECURITY SERVICES AG CLUE	proofpoint.	SoSafe Cyber Security Awareness
Johannes Raff	Oliver Adam	Lukas Schaefer, Geschäftsführer
Angriffe auf Unternehmen mit Hilfe von Phishing häufen sich zunehmend und die Qualität dieser steigt ebenfalls konstant. Unternehmen, welche auf Phishing Simulationen zurückgreifen und ein kontinuierliches Programm verfolgen, trainieren ihre Mitarbeiter stetig und das Bewusstsein über diese persönlichen Angriffe wird gefördert. Phishing Simulationen stellen diese Angriffe nach und halten das Thema für Mitarbeiter aktuell.	Der Mensch ist in der Regel der schwächste Akteur bei der Aufrechterhaltung der Sicherheit, deshalb zielen Hacker auf Menschen und nicht auf Maschinen. Social Engineering ist auf dem Vormarsch und Organisationen müssen darauf angemessen reagieren. Selbst beim Einsatz von hoch entwickelten E-Mail-Schutztools gelangt ein kleiner Teil der schädlichen Nachrichten in die Posteingänge der Anwender. Geschulte Anwender sind entscheidend für das Erkennen und Stoppen von modernen Angriffen. Phishing Security Awareness sind entscheidend für das Erkennen und Stoppen von Phishing-Angriffen.	Phishing-Simulationen lösen den Schulungsinhalt („Wie erkenne ich betrügerische E-Mails?“) aus der abstrakten Darstellung innerhalb klassischer Lernformate und integrieren ihn stattdessen in den Arbeitsalltag. Die Schulung findet genau an dem Ort statt, wo auch echte Angriffe stattfinden: im Posteingang des Anwenders. Wir nennen dies „Lernen am Objekt“. Auch sehen wir, dass die Bereitschaft der Mitarbeiter, sich mit weiteren IT-Sicherheitsthemen auseinanderzusetzen, deutlich steigt, wenn Phishing-Simulationen Teil des Gesamtprogramms zur Sensibilisierung sind. Sie dienen daher als eine Art „Möglichmacher“. Zu guter Letzt sehen wir aber anhand der von uns erhobenen Daten vor allem auch eins: Phishing-Simulationen sind -wenn sie denn richtig umgesetzt werden – ein effektives Mittel, um die Aufmerksamkeit der Mitarbeiter zu erhöhen und das Risiko, auf einen Angriff hereinzufallen, merklich zu reduzieren.
Schulungsmaßnahmen führen nur zum Erfolg, wenn diese in einem kontinuierlichen Konzept geplant und umgesetzt werden Ohne die Messung der Ausführung und Erfolg der Kampagnen, kann die weitere Ausführung nicht an den Bedarf des Unternehmen angepasst werden Da das Bewusstsein und der Umgang mit Kommunikation und Daten in jedem Unternehmen individuell ist, muss durch die Anpassung der Kampagnen auf das jeweilige Unternehmen eingegangen werden, was ohne KPIs nicht möglich sein wird	Assessments, KPIs, Berichte sind ein wichtiger Baustein. Entscheidend für den Erfolg von solchen Maßnahmen ist jedoch das Zusammenspiel von allen Bausteinen und Faktoren. Eine Unternehmenssicherheitskultur kann nur funktionieren, wenn Menschen, Prozesse und Technologien in allen Aspekten eine Berücksichtigung finden. Die richtige Interpretation der Berichte aus den einzelnen Lösungen und eine faire, mitarbeitergerechte Umsetzung der Maßnahmen werden eher zum Erfolg führen, als z.B. das bloße Verfolgen von KPIs.	Zum einen kann damit der Schulungserfolg dokumentiert und auch kommuniziert werden, was Kunden und Mitarbeiter sehr schätzen und z. T. auch für Zertifizierungen (wie z.B. ISO-27001) benötigen. Zum anderen lassen sich aber auch Themen oder Nutzergruppen identifizieren, die intensiver trainiert werden sollten. Ganz wichtig ist aber: Simulationen dürfen keine Überwachungsmaßnahme oder ein „Test mit Blaming“ sein, d.h. eine Auswertung sollte nur auf anonymer Gruppenebene erfolgen. Und die genutzten KPIs müssen klar und einfach verständlich sein; nicht nur für den CISO, sondern auch für Geschäftsführung und jeden einzelnen Mitarbeiter. Künstlich komplizierte Messkonstrukte wie „Sicherheitslevel“ sind hier eher kontraproduktiv.

ELEVATOR PITCH PHISHING (2/2)

Tool/Anbieter	HoxHunt	IT-Seal
Frage 3: Was sind die drei herausragenden Eigenschaften Ihres Tools gegenüber Wettbewerber-Angeboten? Bzw. was ist der USP, wenn ich Ihr Instrument einsetze?	Happy users. Training platform awards the employees about the right kind of behavior. Employees are getting extra awards when accomplishing short extra training moments. Taking into consideration today's fast paced world, it is important to keep the trainings as short, engaging and lightweight as possible. Producing engaging and lightweight training experiences has been seen as one of the key factors in producing behavior change in an organization. Continuous micro-training moments. Hoxhunt's service focuses on positive reinforcement and creating an excellent user experience that becomes part of the day-to-day work. The prerequisites to providing a continuous training model (spaced repetition) is that the user experience is excellent. Employees are getting on average a short training moment every 10 days. Automation. Hoxhunt's automated phishing simulator send attacks that resemble real-life threats. Information security teams can outsource the all the heavy lifting when it comes to creating relevant and recent content for their employees according their according their e.g. skillset, country and language.	1. Spear-Phishing:Wir sind in der Lage, nicht nur Massen- sondern auch gezieltes Spear-Phishing zu simulieren. Dazu sammeln wir zunächst frei verfügbare Informationen aus dem Internet. Häufig handelt es sich dabei um vom Beschäftigten selbst veröffentlichte Informationen. So können wir individuelles Spear-Phishing simulieren – teilweise bis hin zur Nutzung individueller Hobbys und Interessen. Wir senden somit nicht eine E-Mail an 5000 Mitarbeiter, sondern 5000 unterschiedliche E-Mails an 5000 Mitarbeiter in verschiedenen Schwierigkeitsgraden. 2. Messbarkeit: Das Problem bei Klickraten ist die Ungenauigkeit: Durch den Versand von E-Mails in unterschiedlichen Schwierigkeitsgraden und zu verschiedenen Zeiten sind wir in der Lage, eine standardisierte Kennzahl zu berechnen, die das Sicherheitsniveau misst: Den Employee Security Index (ESI®). Durch den ESI können Kunden messen, wie sich das Informationssicherheitsverhalten entwickelt und vergleichen, wie die Gruppen untereinander und die Organisation selbst im Vergleich zu Mitbewerbern dastehen. 3. Awareness-Programm „Lifetime“: Dies ist das Full-Service-Paket von IT-Seal. Mit diesem Programm werden Mitarbeiter in Unternehmen langfristig und nachhaltig für Social-Engineering-Attacken sensibilisiert.
Kurzdarstellung	Hoxhunt is the leading provider of security engagement platforms worldwide. Hoxhunt's security engagement training turns employees into a strong security shield by empowering them with the skills and knowledge to identify and report cyber threats. The Hoxhunt training provides gamified simulation, best-in-class real-time reporting of threats with our unique incident response module to equip security teams with the necessary intelligence to mitigate attacks and breaches faster. Hoxhunt works with Global 2000 organizations from a variety of industries, such as financial services, manufacturing, telecommunication, retail, and much more, to help the customers educate their employees better and thus reduce risk related to human error.	IT-Seal hat sich auf Social Engineering Angriffe und Security Awareness spezialisiert. Ausgezeichnet als Bestes CyberSecurity StartUp auf der it-sa 2018 unterstützt IT-Seal Behörden und Unternehmen aus verschiedensten Branchen wie Maschinenbau, Banken, Behörden oder Krankenhäuser dabei, ihre Mitarbeiter nachhaltig abzusichern. Mit dem Projekt „Bleib wachsam, Darmstadt!“ hat IT-Seal gemeinsam mit der Digitalstadt Darmstadt das weltweit erste kostenlose Awareness-Programm für Bürger und Privatpersonen gestartet. Zudem wird IT-Seal aktuell vom BMBF gefördert, um ein automatisiertes und kennzahlengesteuertes Awareness-Programm namens „Lifetime“ zu entwickeln und so das Thema für die Breite der Unternehmen und Behörden leichter adressierbar zu machen.

Lucy/ Clue Security Service	Proofpoint/Wombat	SoSafe
Lucy Security kombiniert Trainings Inhalte wie auch Phishing Simulationen um bei einer erfolgreichen Simulation direkt auf die Erkennungsmerkmale zu schulen. Phishing Simulationen können in allen Komplexitätslevel ausgeführt werden, um allen Anforderungen an die Mitarbeiter und Bereiche gerecht zu werden. Durch das „Clue Awareness Program“ können Unternehmen die Phishing Simulation und Training als monatlichen Managed Service beziehen, ohne Investitionen und damit ohne hohe Initialkosten ein Awareness Programm für Mitarbeiter einführen.	Unsere Security Awareness Lösung ist marktführend im Gartner Quadranten gelistet. Dies ist natürlich kein USP im eigentlichen Sinn, drückt allerdings aus, dass wir die für den Enterprisemarkt wichtigen Funktionen und Automatismen bieten. Den wesentlichen Unterschied zu allen macht Proofpoint mit seiner nahtlosen Integration in die Security Operative. Anwender können nicht nur trainieren, sie können erlerntes direkt Anwenden und über unseren Phishing-Button verdächtige Mails melden. Diese Meldung wird automatisch überprüft und über ein integriertes Incident Management Tool aus den Mailboxen aller Nutzer entfernt. Dies betrifft z.B. auch bereits weitergeleitete Nachrichten. Proofpoints Angebot verzahnt die Awareness mit den Sicherheitstechnologien. So messen wir beispielsweise mit welchen Methoden welche Mitarbeiter tatsächlich aktuell angegriffen werden und können exakt diese Muster für eine Phish-Simulation nur für die angegriffenen Nutzer verwenden. So fokussieren wir das Training auf die Regionen, die Mitarbeiter und die jeweils aktuellen Methoden. Weiterhin bieten wir integrale Lösungen an, wie Mitarbeiter über Isolationstechnologien stets geschützt klicken können, wenn diese vermehrt gezielt angegriffen werden oder noch nicht ausreichend trainiert sind.	Wir bieten eine dauerhafte und echte „Fire-and-Forget“-Lösung für das Thema Awareness, die unseren Kunden die Arbeit abnimmt und gleichzeitig auf die Bedürfnisse der Mitarbeiter eingeht. So können wir gezielte Attacken simulieren, können die Inhalte der E-Learning Module kundenspezifisch anpassen (Bsp: „Besagt Ihre Passwortrichtlinie 8, 12 oder XX Zeichen?“ etc.) und bieten mittlerweile 13 verschiedene Sprachen an. Unser Tool kommt ohne komplizierte Installation oder Konfiguration aus und bindet keine ohnehin zu dünn besetzten IT-Kapazitäten. Für den Mitarbeiter bieten wir kurzweilige und interaktive Inhalte aus einem Guss, denn IT-Sicherheit finden die wenigsten Nutzer „sexy“... und durch unseren Fokus auf Datenschutz und Anonymität sind auch Betriebsräte und Datenschutzbeauftragte leicht für unsere Lösung zu begeistern. Unser USP: Passgenaues Awareness-Building aus einem Guss – ohne Adminaufwand, aber dafür mit Spaß für die Nutzer.
Clue adressiert die täglich aufkommenden Security Bedürfnisse ihrer Kunden und löst diese mit einer Kombination aus ausgewählten Enterprise Tools, Security Experten und Vereinfachungen für den Kunden. Durch den ausschließlichen Fokus auf IT- und Information Security ist Clue Ihr unabhängiger Security Berater. Durch spezialisierte Security Engineers unterstützen wir Sie bei der Implementerung von Security Produkten und übernehmen auf Wunsch den gesamten Betrieb Ihrer Cyber Defense Infrastruktur. Unser Angebot umfasst Security Consulting, Managed Services und Penetration Testing.	Proofpoint bietet Unternehmen Schutz und Transparenz im Hinblick auf das größte Sicherheitsrisiko – die Mitarbeiter. Wir bieten effektive Sicherheits- und Compliance-Lösungen, um auf Cyber-Angriffe auf jedem Kanal angemessen zu reagieren – einschließlich E-Mail, Internet, Cloud und Social Media.	Die SoSafe GmbH, mit Sitz in Köln und aktuell 35 Mitarbeitern, ist ein auf Awareness-Building spezialisiertes Security-Startup, welches Phishing-Simulationen sowie interaktive E-Learnings zum Thema IT-Sicherheit anbietet. Die mittlerweile über 130 Kunden reichen vom Architekturbüro mit 20 Mitarbeitern über mittelständische „Hidden Champions“ bis zu Bundestagsfraktionen und Großkonzernen wie Vaillant, Ceconomy oder Vattenfall

AUTOREN & HERAUSGEBER

Marcus Beyer unterstützt und berät seit 15 Jahren Unternehmen und Organisationen bei der Umsetzung von Kampagnen zur Sensibilisierung von Security-, BCM- oder Digital Transformation Prozessen. Fokus liegt immer auf einer nachhaltigen Kommunikation und der Interaktion mit Menschen.

***Ankha Haucke**, Diplom Psychologin, Einzel- und Paartherapeutin, qualitative Marktforscherin. Bei known_sense ist sie mit Ivona Matas die Social Engineering-Expertin und u. a. verantwortlich für die Durchführung von tiefenpsychologischen Security-Wirkungsanalysen.*

***Michael Helisch** ist Gründer von HECOM Security Awareness Consulting. Mit Dietmar Pokoyski ist er Herausgeber des einzigen Security Awareness-Fachbuchs in deutscher Sprache. Den Preis Care4Aware hat er gemeinsam mit den TAKE AWARE EVENTS aus der Taufe gehoben.*

***Jean Kolarow**, als stellvertretender CSO eines KRITIS-Betreibers in Berlin beschäftigt er sich vorwiegend mit Sicherheitsstrategie, Krisenmanagement und Security Awareness. In seinem Zweitstudium an der RFH Köln spezialisierte er sich auf das Thema Compliance und deren übergreifende Kommunikation.*

***Lotta Krickel** ist studierte Medienpädagogin und unterstützt das Actionbound-Team mit ihrer jahrelangen praktischen Erfahrung in Gamification, Game Design, Storytelling und emotionalem Lernen. In Workshops und individuellen Consultings erklärt sie unseren Kunden aus Unternehmen und Bildungsinstitutionen, wie sie ihre Lerninhalte kreativ vermitteln können.*

***Dietmar Pokoyski**, Geschäftsführer der Awareness-Agentur known_sense und gemeinsam mit Michael Helisch Herausgeber des einzigen Fachbuchs zum Thema in Deutschland. Seit 2005 hat er zahlreiche Awareness-Games und Kampagnen kreiert bzw. als Trainer und Supervisor Game Based Security Events in 60 Ländern und 30 Sprachen durchgeführt bzw. begleitet. Mit known_sense erhielt er zahlreiche Auszeichnungen, u. a. den „IT-Sicherheitspreis NRW“ (2007) sowie den „OSPA – Oustanding Security Performance Award“ (2015) für eine herausragende Initiative für Sicherheitsschulungen. Pokoyski ist außerdem mit Uwe Röniger Co-Produzent der TAKE AWARE EVENTS und Mitherausgeber dieses Magazins.*

***Uwe Röniger**, Geschäftsführer der mybreev GmbH und ein erfahrener Spezialist bei der Entwicklung unternehmensspezifischer E-Learning Programme, verantwortet die Gesamtentwicklung von 300 B2B-Schulungsprojekten und Kampagnen, darunter zahlreiche Kommunikationsprojekte für DAX-Konzerne mit der Koordination fachübergreifender Teams auf nationaler und globaler Ebene. Aktuell produziert er u. a. das Gesamtprogramm von Corporate Security TV (CSTV) und mit Dietmar Pokoyski das der TAKE AWARE EVENTS.*


AWARE
HOUSE
MEISTER
SEXY SECURITY

BLUFF CITY 2021 # 03

MANIPULATION, DESINFORMATION & CO. ALS INFORMATIONSSICHERHEITSRISIKEN

Die Social Engineering Konferenz

MOTTO: »SCHLECHTE VERSTECKE – DEEP FAKES, DOXING & CO.«

BERLIN | HERBST 2021

DEUTSCHES SPIONAGEMUSEUM

FEAT. CEO-FRAUD | PHISHING | HUMAN HACKING | FORENSIK | FAKE NEWS | HUMAN EXPLOITS

MUSEUMSFÜHRUNG & GRATISEXEMPLAR TAKE AWARE SEC&LIFE MAGAZINE #04

Konferenz-Veranstalter

BSKI Bundesverband für den Schutz Kritischer Infrastrukturen e.V.

DEUTSCHES SPIONAGE MUSEUM GERMAN SPY MUSEUM

my breev

known_sense awareness you can touch.

Netzwerkpartner

ASIS INTERNATIONAL ASIS GERMANY e.V.

Medienpartner

CORPORATE-SECURITY.TV

<kes> Die Zeitschrift für Informations-Sicherheit

SecuMedia Der Verlag für Sicherheits-Informationen

BLUFF CITY 2021 BERLIN Die Social Engineering-Konferenz

www.bluff-city.net