TAKE AWARE

SEC&LIFEMAGAZINE

EDITION TAKE AWARE 04

SONDERTEIL: DIE 3 GEWINNER 2020

Care4Aware
Der Security Awareness-Award

MOTTO: »INTERNE KOMMUNIKATION & CORONA – AWARENESS HALB UND HALB?«

CARE4AWARE: SO SEHEN SIEGER AUS | PITCH: GOOD COVID-PRACTICE VON AMADEUS – COMMERZBANK – IWC SCHAFFHAUSEN – RWE – SWITCH | PODCAST: »SECURITY AWARENESS INSIDER« | INTERVIEW MIT FABULA GAMES: GAMIFICATION BRAUCHT EINE STORY | DIE VISION VOM SICHEREN UNTERNEHMEN | CHRIS SCHOG – OSPA FÜRS LEBENSWERK | NIEMAND IST ANONYM | INKOHÄRENZ & VERLETZLICHKEITS-PARADOX | DAS ANGST-DILEMMA DER AWARENESS

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

mybreev

known_sense
awareness you can touch.

Medienpartner

CORPORATE SECURITY.TV

AUCH BEI PRIVACY KEINE HALBE SACHEN

SCHUTZ DER PRIVATSPHÄRE – GERADE ZUHAUSE FÜR FUNKTIONIERENDE PAARBEZIEHUNGEN IMMER WICHTIGER

TAKE AWARE
SECLIFEMAGAZINE
04

SECURITY IMAGE: JEDER INCIDENT IST EIN WERTVOLLER KONTAKT

Liebe Leser, verehrte Awareness-Freunde,

während der Pandemie häuften sich in den sozialen Netzwerken Frustrations-Posts von InfoSec-Kollegen und -Kolleginnen, die behaupteten, alles würde infolge von Corona „schlimmer werden", die Risiken würden zunehmen, ein Sich-gehen-lassen im Homeoffice mit der „Unterwanderung" von Sicherheitsmaßnahmen wäre state-of-the-art, Remote-Settings würden die Gefahren von Informationsverlusten fördern. Wir wollen das hier nicht direkt bewerten, aber beispielhaft und kurz auf einen Diskus mit einem Kollegen auf LinkedIn eingehen, der konstatierte, Informationssicherheit würde ein extrem schlechtes Image zugeschrieben werden, niemand würde sich „wirklich dafür interessieren". Nun ist Fatalismus eine bequeme Umgangsform mit der eigenen Frustration und temporär sicher akzeptabel, um sich selbst vor allzu harten Abstürzen zu bewahren. Wir können diese These jedoch nicht so stehenlassen. Die steigende Anzahl von Fehlleistungen bis hin zu Incidents belegt doch, dass Menschen sich sogar sehr intensiv mit dem Thema Informationssicherheit konfrontieren. Und ein Incident schließt eine anschließende Beschäftigung mit dem Vorfall ja nicht per se aus. Auch wenn die Beschäftigung mit Sicherheitsmaßnahmen oft unbewusst abläuft, haben sich noch nie so viele Menschen mit dem Thema beschäftigt. Eine Feststellung, man würde sich nicht dafür interessieren, ist mithin allein' aus tiefenpsychologischer Sicht unhaltbar; vielmehr belegt jede einzelne Fehlleistung das hohe Interesse am Thema. Und eine aktive Veränderung durch Modellierung der Sicherheitskultur infolge von z.B. Security Brand Management, Security Marketing oder Awareness stärkt das Image der Sicherheitsbereiche, ihrer Protagonisten und des Themas generell. So nachzulesen in unserer Corona-Umfrage zum Thema ab Seite 24, aus der heraus das Thema „Awareness halb & halb" deutlich wird, nämlich dass digitale Tools temporär zur Sensibilisierung funktionieren, jedoch Awareness nicht komplett ist, wenn die direkte Beziehung nicht permanent warm gehalten wird. Auch die rege Beteiligung mit den guten bis sehr guten Beiträgen im Rahmen unseres Awareness-Wettbewerbs „Care4Aware" belegt den zunehmend aktiven Umgang mit Sicherheitskultur und -image. Die infolge von Corona „verspäteten" Sieger finden Sie ab Seite 15. Darüber hinaus haben wie immer mit dieser Ausgabe ein umfangreiches und höchst diverses Awareness-Kompendium geschaffen, aus dem Sie hoffentlich zahlreiche Anregungen mitnehmen wollen und werden. TAKE AWARE. TAKE AWAY. TAKE CARE.

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

CONTENT

Podcast: »Security Awareness Insider« *von Katja Dörlemann & Marcus Beyer | S. 04*

Fabula: Gamification braucht eine Story – Interview mit Eric Fleury & Tomislav Bodronzic *| S. 06*

Die Vision vom sicheren Unternehmen *von Uwe Röniger, Vladyslav Moyerer & Markus Wagemann | S.10*

Care4Aware – das sind die Gewinner 2020 *von Michael Helisch & Dietmar Pokoyski | S. 14*

Niemand ist anonym –Täter anhand ihrer Sprache identifizieren *von Steffen Hessler | S. 18*

Miniposter »Connected Car Security« *| S. 22*

»Biedermeier« oder »Ich will hier raus?« – Corona-Umfrage *| S. 24*

Awareness-OSPA statt „Sensiblisierungs-OPA" Auszeichnung für Chris Schog *von Dietmar Pokoyski | S. 34*

Inkohärenz & Verletzlichkeitsparadox *von Dietmar Pokoyski | S. 36*

Das Angst-Dilemma in der Awareness *von Dietmar Pookoyski | S. 38*

Die Autoren & Herausgeber *| S. 40*

PODCAST: »SECURITY AWARENESS INSIDER«

VON KATJA DÖRLEMANN & MARCUS BEYER

Klick. Rauschen.

KATJA: *räusper* Test, Test...*räusper* Test. Läuft.

MARCUS: Gut, dann fang ich mal an. Hallo Katja, schön, dass Du da bist.

KATJA: Hallo Marcus, dito!

MARCUS: Heute geht's um unseren „Security Awareness Insider"-Podcast.

KATJA: Genau. Wo fangen wir am Besten an?

MARCUS: Vielleicht ein bisschen mehr Kontext? Erzähl' mal, worum's geht.

KATJA: Stimmt. Also. In dem Podcast sprechen wir mit anderen Expert/innen über Security Awareness, Mitarbeitersensibilisierung, neue und kreative Wege, Tools, Trainingsansätze, Insights in Programme von Unternehmen und Organisationen und noch viel, viel mehr.

MARCUS: Ein Mix aus Theorie und Praxis. Davon kann man sich in den ersten Folgen schon überzeugen. Und eben, viele Insights auch in Bereiche und Themen, die man nicht zwangsläufig mit Security in Verbindung bringt...

KATJA: Storytelling...

MARCUS: Psychologische Faktoren...

KATJA: IT-Kommunikation...

MARCUS: Und mehr. Das war und ist schon spannend – und macht's vielleicht hier und da auch komplex. War ja auch das Thema unserer ersten Folge: „Warum ist das alles so kompliziert?".

KATJA: Genau. Aber Marcus?

MARCUS: Ja?

KATJA: Wie kommt man denn auf die verrückte Idee einen Podcast über Security Awareness zu machen?

MARCUS: Kennst mich doch. *lacht* Fiel mir unter der Dusche ein, da habe ich ganz oft ganz kreative Ideen, kennt man ja. Und dann habe ich die Idee mal im September auf LinkedIn gepostet und bam! – 44 Likes, 41 Kommentare und über 5.100 mal angeschaut. Da habe ich mir gesagt, da ist Bedarf da... und da isser. Mit Dir. Und Gästen. Ich finde das großartig.

KATJA: Ja, ich auch! Es ist aber auch schräg.

MARCUS: Was ist schräg?

KATJA: Es gibt tausendundeinen Podcast über Cyber Security, aber kaum einen über Security Awareness.

MARCUS: Eben! Das musste geändert werden.

KATJA: Gut, dass Du duschen gehst.

MARCUS: *lacht* Ja... Das Feedback zu unseren ersten Folgen bestätigt das auch.

KATJA: Das ist durchweg positiv! So eine halbe Stunde Security Awareness-Input im Monat tut scheinbar allen Awareness-Freund:innen da draußen gut.

MARCUS: Hat schon was von Sebsttherapie – auf allen Seiten. *lacht*

KATJA: *lacht* Oh ja.

MARCUS: Und wir haben noch so viele Ideen und so viele großartige Expert/innen in petto.

KATJA: Definitiv! Unserer Hörer/innen können sich schon jetzt auf weitere spannende Gespräche freuen.

MARCUS: So sieht's aus. Aber Katja?

KATJA: Ja?

MARCUS: Wann kommt nochmal die nächste Folge raus?

KATJA: Wie immer, am letzten Mittwoch des Monats.

MARCUS: Ah ja, stimmt. Wer macht den Ton?

KATJA: Mike Bichsel. Wer hat uns den Jingle gemacht?

MARCUS: Jakob Dhondt. Und wer orchestriert die Tech-Magie hinter allem?

KATJA: Der wunderbare Oli Schacher!

MARCUS: Yeah! So. Dann sagen wir mal „Tschüss", oder?

KATJA: Gute Idee. Bis zum nächsten Mal in unserem Podcast, liebe Leser/innen!

MARCUS: Machs guet. Mir ghöre üs und bis gli, liebe Hörer/innen!

Rauschen. Klick.

Oli: Tip Top, Leute. Wir haben alles.

«Security Awareness Insider» mit Marcus und Katja erscheint monatlich immer am letzten Mittwoch.
Hört rein:

- *https://www.securityawarenessinsider.ch/*
- *https://open.spotify.com/show/2yh47EAnxYyp63rbkfIHDb*

FABULA: GAMIFICATION BRAUCHT EINE STORY

INTERVIEW MIT ERIC FLEURY (UNT. L.) & TOMISLAV BODROZIC, GRÜNDER VON FABULA GAMES

FRAGEN VON DIETMAR POKOYSKI

Fabula Games ist Experte für digitale Weiterbildung mithilfe von Serious Games bzw. Gamification, u. a. im Bereich Informationssicherheit und Datenschutz. Seit Anfang 2021 existiert eine Kooperation von Fabaula Games mit den Herausgebern dieses Magazins, known_sense und mybreev.

Eric, Tomislav, würdet ihr euch bitte kurz vorstellen? Was ist euer Hintergrund und wie seit ihr zum Thema Spiel gekommen?

Eric Flury (EF): Ich habe mehr als 20 Jahre lang als Gründer und Manager einer großen Personalberatungsfirma in der Schweiz gearbeitet. In dieser Funktion konnte ich die Bedeutung von Mitarbeiterschulungen messen und auch erkennen, welche enorme Investition eine Präsenzschulung darstellt und wie schwierig es ist, diese Schulung für die Mitarbeiter motivierend zu gestalten. Auf halber Strecke meiner Karriere hatte ich Lust, etwas Neues zu beginnen und schloss mich Fabula Games an, das mein langjähriger Freund Tomislav kurz zuvor gegründet hatte.

Tomislav Bodrozic (TB): Ich habe Psychologie studiert und dann die Liebe zum Film entdeckt. Dort habe ich 15 Jahre lang als Redakteur und Regisseur gearbeitet – bis ein großer Kunde ein Serious Game von uns haben wollte. Das war der Beginn von Fabula Games, und für mich die Legitimation, nicht nur in der Freizeit zu spielen, sondern jeden Tag und jederzeit.

Spielt ihr persönlich spiele, wenn ja welche und in welchem Umfang?

EF: Ich bin das, was man einen Gelegenheitsspieler nennen könnte. Ich spiele, wenn mich ein Freund einlädt, vor allem aus Freude am Wettkampf.

TB: Ich spiele jeden Tag. Sowohl Casual Games, die nur 2-3 Minuten pro Level dauern, als auch epische Spiele von seeeehr langer Dauer.

Wie ist es zur Gründung von Fabula Games bzw. wie zu eurer Zusammenarbeit gekommen? Gab es ein initiales Ereignis? Wofür genau steht das Wording bei FABULA als Marke?

TB: Die ersten Spiele haben ich mit der Firma Fabula Film entwickelt, wo ich viele Jahre als freier Mitarbeiter tätig war. Irgendwann war die Zeit reif, um die Serious Games aus dem Filmagentur-Geschäft auszugliedern. Bei den Spielen handelt es sich um ein grundsätzlich anderes Produkt als bei Filmen. Und so haben wir beschlossen, die Firma Fabula Games zu gründen. Übrigens kommt das Wort Fabula aus dem Lateinischen und bedeutet „Geschichte“. Und genau die braucht jeder gute Film – und jedes gute Spiel.

Ihr fasst eure Games als Teil von E-Learning zusammen. Wie definiert ihr E-Learning? Wer sind eure Wettbewerber, warum und wie unterscheidet ihr euch?

TB: Wenn man es sehr wörtlich nimmt, dann bedeutet E-Learning nichts anderes als dass Lerninhalte elektronisch, also digital statt analog vermittelt werden. Also am Computer, Tablet oder Smartphone. Allerdings gehen wir einen deutlichen Schritt weiter: unsere Entwicklungen gehören zu der Gattung der Game-based Learnings, also zum spielebasierten Lernen. Der unterscheidet sich maßgeblich vom herkömmlichen E-Learning, das lediglich den Fokus auf die Wissensvermittlung setzt. Wir versuchen, die Lernenden zu unterhalten, Spaß zu vermitteln, Freude zu machen und so zu motivieren. Und außerdem gibt es ein grundlegend anderes didaktisches Lernkonzept dahinter.

EF: Ich kann für den zweiten Teil antworten. Unsere Hauptkonkurrenten sind Unternehmen, die Serious Games auf Katalogbasis entwickeln, wie Gamelearn (Spanien) oder Daesign (Frankreich). Darüber hinaus gibt es eine große Anzahl von Unternehmen, die Serious Games als Einzelprojekte entwickeln. Die meisten von ihnen tun dies neben anderen Aktivitäten. Fabula Games entwickelt ausschließlich Serious Games, als Projekt oder als Katalog, was uns ziemlich einzigartig macht.

Wie seit ihr zum Thema Informationssicherheit gekommen? Was ging euch als erstes durch den Kopf, nachdem ihr von ten4 consulting in Bezug auf das Projekt bei Bayer angesprochen wurdet. Welche Herausforderungen bzw. Barrieren gab es im Kontext der Spielentwicklung? Wie habt ihr euer Know-how-Vakuum in Bezug auf Informationssicherheit gefüllt bzw. ausgeglichen? Wie erging es euch dabei, euch dem Thema Informationssicherheit zu nähern?

TB: Das Serious Game „The SECRET of Photonorvin” war eines der spannendsten Projekte überhaupt. Wir mussten uns die für uns neue Thematik Informationssicherheit einarbeiten, und wurden dabei großartig unterstützt von der Unternehmensberatung ten4. Das Spiel sollte eine langfristige Awareness-Maßnahme für Bayer-Mitarbeiter sein. Das Game Design musste also über mehrere Monate hinweg für Neugier sorgen und die Mitarbeiter motivieren, sich dem Spiel weiter zu widmen. Der Kniff dabei war es, ein episches Story-Adventure-Game zu entwickeln, das ähnlich wie gut gemachten Serien mit Cliffhangern arbeitet und Spannung aufbaut. Das war der Clou bei dieser Produktion. Und natürlich, dass es von Grund auf ganz speziell für diesen einen Kunden entwickelt werden konnte, was uns eine Menge Spaß gemacht hat.

Wenn Informationssicherheit eine Farbe hätte, welche wäre die und warum?

EF: Für mich ist es eine Mischung aus Blau und Rot. Blau, weil das Feld rational ist und von den Mitarbeitern oft als langweilig empfunden wird. Und rot, denn wenn man nicht aufpasst, kann man sich die Finger verbrennen und alle möglichen Emotionen durchleben.

Wie sah euer Kundenportfolio aus, bevor ihr MYRO P7 gelaunched habt und wie hat er sich durch MYRO P7 verändert?

TB: Vor myRo P7 haben wir ausschließlich auf Bestellung eines Kunden individuelle Serious Games

entwickelt. Das hat den Vorteil, dass wir das Spiel exakt so designen konnten, wie es am besten für die Inhalte und den Kunden funktioniert. Hat aber auch den Nachteil, dass es ein relativ hoher Aufwand ist.

EF: myRo P7 war das erste Spiel in diesem Feld in unserem Portfolio von Katalogspielen. Seitdem haben wir ein Spiel für Reisesicherheit, und ein Spiel für Sicherheit zu Hause entwickelt. Unser neuestes Produkt heißt „Social Engineering Trap“ und zielt, wie der Name schon sagt, vor allem auf die Sensibilisierung der Mitarbeiter für solche Risiken ab.

Hattet ihr persönlich bei Fabula oder woanders jemals mit Security Awareness-Maßnahmen, z. B. als Zielgruppe, zu tun?

EF: Nein, in meiner alten Firma hatten wir keine speziellen Maßnahmen. Natürlich versuchen wir, den Markt regelmäßig zu scannen, um zu sehen, was andere Anbieter machen. Als kleines Unternehmen müssen wir jedoch zugeben, dass dies nicht systematisch ist.

Welche anderen Awareness-Kampagnen/-Tools kanntet ihr, als ihr wg. MYRO P7 gefragt wurdet? Habt ihr eine Wettbewerber-Analyse durchgeführt?

TB: Bei unseren regelmäßigen Marktuntersuchungen sind wir auf viele Wettbewerber gestoßen (übrigens auch auf e-sec – nur hat Eric das wahrscheinlich vergessen ;-)). Wir versuchen uns jedoch nicht einnehmen zu lassen von den Ansätzen anderer, sondern suchen unseren Weg, bei dem wir unseren Stärken am besten einbringen können.

Wie würdet ihr Security Awareness definieren? Was sind die Erfolgsfaktoren einer Kampagne?

EF: Security Awareness ist für uns das Schaffen eines Bewusstseins und die Sensibilisierung der Mitarbeiter für die Risiken. Meiner Meinung nach ist eine Kampagne dann erfolgreich, wenn die Mitarbeiter mit den potenziellen Risiken konfrontiert werden, diese erkennen, die möglichen Konsequenzen einschätzen können und ihr Verhalten entsprechend anpassen oder ändern.

Was sind die Schwächen von Awareness-Maßnahmen, die euch ggf. bekannt sind? Mit welchen Stärken und Schwächen würdet ihr MYRO P7 (oder die neuen Security Games) in Zusammenhang bringen?

EF: Die größte Schwäche klassischer E-Learnings ist das fehlende Eintauchen in den Lernkontext. Dabei wird meist nur kognitiv gelernt und verarbeitet. Im Normalfall lernen die Mitarbeiter dabei nur 10% von dem, was sie lesen. Ein Serious Game wie myRo P7 versetzt den Mitarbeiter in die Rolle eines Charakters, der eine große Mission hat und sich Cyber-Risiken stellen muss. Je nachdem, wie der Spieler sich entscheidet, kann dies schwerwiegende Folgen für ihn, sein Unternehmen und sogar für die Menschheit haben. Diese Form des Lernens stellt sicher, dass die Mitarbeiter emotional und aktiv in das Training einbezogen werden. Studien zeigen, dass die Lerneffektivität bei 90% liegt – statt bei 10% beim reinen Lesen!

Welche Erfahrung habt ihr in Bezug auf die Awareness-Kampagne bei Bayer gemacht, welche andere Erfahrungen im Nachgang dieser Premiere mit Kampagnen bei anderen Kunden bzw. mit welchen Erfahrungen bzw. Ergebnissen?

TB: Die Bayer-Auftraggeber waren mit unserer Kampagne sehr zufrieden. Leider gibt es keine Zahlen über die Beteiligung, weil das aus Datenschutzgründen nicht erfasst werden durfte. Die Rückmeldungen zu diesem Serious Game hat uns veranlasst, mit myRo P7 unsere eigene Version eines InfoSec Serious Games zu entwickeln – übrigens wieder zusammen mit ten4 consulting. Damit machen wir es auch KMUs und Mittelständlern möglich, ein Serious Game zu diesem Thema zu nutzen, da hier nur Lizenzgebühren und keine vollen Entwicklungskosten entstehen.

Warum habt ihr weitere Informationssicherheits-Games kreiert? Gab es Kundenanfragen als Treiber. Welche Erfahrungen konntet ihr aus MYRO P7 in die Neuprodukte mitnehmen?

EF: Wir haben schnell erkannt, dass nicht alle Kunden die gleichen Erwartungen haben. Manche bevorzugen ein Spiel, das alle Themen abdeckt, andere wollen ein spezifischeres Training. Einige Kunden haben uns gesagt, dass das große Abenteuer, das wir in myRo P7 gesteckt haben, nicht zu ihrer Unternehmenskultur passt. Aus diesem Grund entwickeln wir ein Portfolio von Serious Games im Bereich Sicherheit.

Wie geht ihr an ein Security Game methodisch heran? Geht ihr von einem Thema aus? Von einem Narrativ?

TB: Wir versuchen, mit dem Portfolio jeweils unterschiedliche Ansätze bei den einzelnen Spielen zu integrieren. So ist zum Beispiel unser neues Spiel „SET – Social Engineering Trap“ entstanden, das nur ein ungewöhnliches Setting verwendet, anstatt eine epische Geschichte zu erzählen. Spielt sich schneller und direkt; so dass Unternehmen nun wählen können, was besser zu ihnen passt.

Wie geht ihr in den Vertrieb der Security Produkte? Was sind die Besonderheiten der Security Branche?

EF: Als Entwickler von Serious Games haben wir kein besonderes Netzwerk mit Sicherheitsverantwortlichen. Deshalb setzen wir auf Partner, die auf diesem Gebiet spezialisiert sind. Parallel dazu versuchen wir, im Internet so sichtbar wie möglich zu sein, so dass CISOs, ISOs und IT-Manager, die nach einer Lösung suchen, uns leicht finden können.

Ihr produziert die Games mit einem bestimmten Game Creator. Welcher ist das, wie seit ihr darauf gekommen und warum habt ihr euch für diesen und nicht für ein Wettbewerber-Produkt entschieden?

EF: Wir sehen den Kern unseres Berufes mehr von der pädagogischen und didaktischen Seite als von der technischen Seite. Aber wir wollen trotzdem die Kontrolle über den gesamten Produktionsprozess haben. Deshalb haben wir nach dem idealen Tool gesucht, mit dem wir die von uns produzierten Konzepte effektiv entwickeln können. Es war eine lange Suche, aber wir haben mit dem VTS Editor der französischen Firma Serious Factory ein sehr zufriedenstellendes Werkzeug gefunden. Und sind mittlerweile auch eine Partnerschaft mit dem Herausgeber dieser Lösung eingegangen, den wir in der DACH-Region vertreten.

Welche Themen wollt ihr zukünftig angehen? Was ist in der Pipeline?

TB: Unser aktuelles Serious Game zum Thema Social Engineering heißt „SET – Social Engineering Trap“. Darauf sind wir mächtig stolz, weil es eine komplett andere Herangehensweise ist.

EF: Und unsere nächste Entwicklung wird voraussichtlich zum Thema DSGVO sein.

TB: Darüber hinaus arbeiten wir ja ständig an Kundenprojekten, also an individuellen Produktionen. Die sind immer recht zeitaufwändig …

In der Awareness sind in den letzten 2,3 Jahren einige neue Player vermeintlich „groß“ geworden, die so blind agieren, als wolle man da was hochziehen, was dann schließlich meistbietend vertickt wird. Stichwort: „Awareness als Tool“, z. B. Phishing-Simulationen. Wie steht ihr hierzu? Was, wenn ein Großer mit dem Scheckheft winkt? Tomislav, nimmst du das und kümmerst dich dann z. B. noch mehr um dein Hobby mit den Bienen – oder wäre das nicht reizvoll?

TB: Eigentlich bin ich davon recht unbeeindruckt. Wir können und wollen uns gar nicht mit den großen Anbietern vergleichen, und wir haben das auch nicht vor. Unser Anliegen ist es, möglichst effektive digitale Trainings und Kampagnen zu entwickeln, die Lernen wieder zu einem Abenteuer machen. Wenn das andere auch hinbekommen, dann profitieren die Lernenden davon. Und wenn Lernen wieder Spaß macht, dann sind wir unserer Mission einen Schritt näher. Sollte das jemand besser machen als wir, dann kann er uns kaufen. Ansonsten nicht ;-)

Wie seht ihr E-Learning 2030? Welche Entwicklung wird Security Awareness bis 2030 nehmen? Wo steht Fabula Games 2030?

TB: Digitales Lernen wird sich immer immersiver, das heißt: es wird zu einem ganzheitlichen Erlebnis für die Lernenden. 2030 werden alle mit Brillen/Gläsern lernen, die ein Erleben im Sinne von Augmented Reality und Virtual Reality ermöglichen. Dann wird es selbstverständlich sein, dass wir in diese Lernwelt eintauchen, interaktiv mit anderen gleichzeitig lernen und mit allen Sinnen. So macht lernen nicht nur Spaß, sondern ist auch noch um ein Vielfaches wirksamer und effektiver.

EF: Wir planen, einen echten Awareness-Lehrgang für Mitarbeiter zu entwickeln. Unternehmen können sich anmelden und haben die Gewissheit, dass jeder Mitarbeiter diesen Weg das ganze Jahr über geht. Natürlich immer auf eine unterhaltsame und immersive Art und Weise.

Sucht ihr noch nach Verstärkung? Wenn ja, was müsste ein Bewerber mitbringen?

EF: Ja, wir sind derzeit auf der Suche nach Game Designern. Also immer her mit interessanten Bewerbungen.

Und wenn jemand eine Idee für ein Security Game hat, kann er dann zu euch kommen? Wie geht es dann weiter?

EF: Ja, unbedingt!

TB: Wir sind immer offen für neue Ideen und Vorschläge, die einen Mehrwert bieten. Wir können schnell und sicher einschätzen, ob und wie Kunden davon profitieren würden. Und können dann gemeinsam analysieren, was nötig wäre und wie eine Umsetzung aussehen würde. Meist dauert es nicht lange, um eine Entscheidung zu fällen.

DIE VISION VOM SICHEREN UNTERNEHMEN

EINE DIGITAL SENSIBILISIERTE BELEGSCHAFT

Uwe Röniger, Vladyslav Moyerer, Markus Wagemann

Unternehmen von heute strahlen durch ihren immer offeneren Außenauftritt einen gewissen Grad an Sicherheit und Sicherheitsbewusstsein aus. Dies wirkt sowohl nach innen als auch nach außen, was bedeutet; strahlt das Unternehmen Sicherheit aus, so erzeugt es eine positive Wirkung auf sein Umfeld – und zwar in der Rolle als verantwortungsvolle Institution gegenüber der Gesellschaft, vertrauensvoller Partner aber auch als attraktiver Arbeitgeber. Doch was macht ein sicheres Unternehmen heute aus? – Einen Teil deckt bereits die kontinuierliche Sensibilisierung der Belegschaft zu Vielfältigen Themen ab. Sie ist Bestandteil einer professionellen und zeitgemäßen internen Kommunikation.

1. Sicherheit im Unternehmenskontext – die Herausforderungen wandeln sich

Jedes Zeitalter birgt seine spezifischen Risiken für die arbeitenden Menschen. Sich diesen zu stellen, sie zu minimieren und das passende Werkzeug für den korrekten Umgang mit diesen zu finden stellt seit jeher eine wichtige Aufgabe der jeweiligen Generationen dar. Eines der hierbei verfolgten Ziele zieht sich über Jahrhunderte hindurch; die Menschheit strebt nach dem Grundbedürfnis „Sicherheit“.

Äquivalente Herausforderungen finden sich heute im Unternehmenskontext wieder, auch wenn es oftmals nur unterbewusst passiert. Jedes Unternehmen bewegt sich in einer Sphäre mit spezifischen Anforderungen und Risiken. Definiert wird diese über die Märkte, Politik, die staatlichen Anforderungen aber auch die gesellschaftlichen Aspekte, die sich in der sozialen und ökologischen Verantwortung äußern. Innerhalb von diesem Bewegungsraum beschäftgt die meisten Unternehmen die Frage: „Wie lassen sich die Unternehmensziele, in Anbetracht der unterschiedlichen Risiken, erreichen und ein möglichst sicheres und nachhaltiges Geschäft aufbauen?“

Neben einem funktionierenden, operativen Geschäftsablauf sowie der Verfolgung der ökonomischen Unternehmensstrategien und Ziele, bildet die Unternehmenssicherheit den Rahmen unternehmerischen Handelns. Sie dient der „Sicherung des Geschäftsablaufs und der Prozesse“ und wandelt sich mit der Zeit in Richtung des Notfall-, Krisen- und Risikomanagements.[1]

Doch bei der Betrachtung der unternehmerischen Risiken darf der einzelne Mitarbeitende nicht aus den Augen geraten. Denn hinter jedem unternehmerischen Ziel, Prozess und letztendlich dem Erfolg stehen Menschen. Wenn also von der Unternehmenssicherheit oder dem Sicherheitsmanagement die Rede ist, so wird in der letzten Konsequenz der Mensch, den es betrifft, betrachtet. „Das Unternehmen muss den Menschen dienen.“[2] – fasst Unternehmer Heinrich Deichmann den Firmenzweck des größten Schuhherstellers Europas „Deichmann SE“ zusammen. Dieser Zweck solle sowohl den Mitarbeitenden als auch den Menschen außerhalb der Organisation dienen. Folglich muss auch die Unternehmenssicherheit den Menschen in den Mittelpunkt stellen.

In einer zunehmend digitalisierten Gesellschaft bleiben viele Risiken aus der vordigitalisierten Zeit bestehen. Dazu gehört der Arbeits- und Brandschutz, die Wirtschaftskriminalität und auch der rechtliche Rahmen, den es einzuhalten gilt. Jedoch prosperieren auch neue Gefahren, die in der digitalen Umgebung ihr natürliches Habitat gefunden haben und durch die Corona-Situation um ein Vielfaches beschleunigt werden. So gewinnen, mit der steigenden Popularität des Home Offices, Themen wie die Cyber Sicherheit, Datenschutz oder Informationssicherheit weiter an Bedeutung. Auch die mentale Gesundheit der Mitarbeitenden und die Nachhaltigkeit des Unternehmens in Bezug auf die Umwelt rücken in den Fokus. Und die Vertiefung der Themen rund um die Gleichberechtigung und Diversität in Organisationen erhalten nun ihre seit Jahren fällige Daseinsberechtigung im Unternehmenskontext.

All diese Risiken gilt es für Unternehmen bei der Definition der eigenen Strategie einzukalkulieren und entsprechende Maßnahmen zu deren Vorbeugung einzuleiten. Doch wie ist es heute möglich, all diese Aspekte zu berücksichtigen, die verschiedenen Themen zu schulen und kontrolliert Sensibilität für diese Gefahren zu schaffen?

2. Grundlagen schaffen – Mitarbeitende digital aufklären

Die Vision vom sicheren Unternehmen kann nicht ohne die Einbindung des Mitarbeitenden entwickelt und realisiert werden. Die IT-Sicherheit offenbart dies eindrucksvoll: „If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.“[3] – lautet ein berühmtes Zitat des Experten für Kryptographie Bruce Schneier. Damit bezieht er sich auf den Fakt, dass der größte Teil von IT-Vorfällen und Datenpannen dem menschlichen Verhalten entspringen. Dies lässt sich ebenfalls auf andere Unternehmensrisiken übertragen.

Dabei ist der Mitarbeitende sowohl der Absender als auch der Rezipient der Sicherheit. Einerseits trägt er selbst zur Sicherheit im Unternehmen bei. Andererseits sehnt er sich nach ihr. So zeigt eine Studie der Personalberatung „Academic Work“, dass die Stabilität des Unternehmens und die damit verbundene Sicherheit eine immer größere Rolle bei der Berufswahl der Young Professionals einnimmt.[4] Dies deckt sich mit einer repräsentativen Umfrage der ZEIT zum Thema Erwartungen und Zufriedenheit am Arbeitsplatz. Die Umfrage zeigt, dass für 83% der 1000 Befragten ein zukunftssicherer Job besonders wichtig ist. Die langfristige Sicherheit des Arbeitsplatzes nimmt mit 82% einen hohen Stellenwert ein.[5]

1 *Unternehmenssicherheit, in: Industrie und Handelskammer zu Leipzig [online], https://www.leipzig.ihk.de/unternehmen/geschaeftsfelder/standortpolitik/sicherheit-in-der-wirtschaft/unternehmenssicherheit/, [05.01.2021]*

2 *Deichmann, Heinrich: Das Unternehmen muss den Menschen dienen, in: Wirtschaftsforum Interview [online], https://www.wirtschaftsforum.de/interviews/das-unternehmen-muss-den-menschen-dienen [05.01.2021]*

3 *Preface, in Schneier Website [online]: https://www.schneier.com/books/secrets-and-lies-pref/ [07.01.2021]*

4 *Krise ändert Job-Prioritäten junger Arbeitnehmer, in personalwirtschaft.de, 03.12.2020, [online] https://www.personalwirtschaft.de/recruiting/artikel/corona-krise-aendert-jobprioritaeten-junger-arbeitnehmer.html [07.01.2021]*

5 *Was wünschen sich die Deutschen von ihrer Arbeit?, in ZEIT Online, 3.12.2018, [online] https://www.zeit.de/2018/50/arbeitnehmer-berufsleben-erwerbstaetigkeit-zufriedenheit-themen-2019-umfrage?utm_referrer=https%3A%2F%2Fwww.google.com%2F [07.01.2021]*

Diese wechselseitige Beziehung zeichnet ein beidseitiges Bedürfnis für eine Unternehmenskultur, bei der die Sicherheit eine feste Größe ist. Dieses Bedürfnis mündet in einer Pflicht für Unternehmen und Mitarbeitende, Sicherheit zeitgemäß zu definieren, sich den Themen der Risikominimierung anzunehmen und diese Themen der Belegschaft zugänglich zu machen.

Doch das Bedürfnis nach Sicherheit geht nicht zwangsläufig mit dem Interesse an der Thematik einher, ganz im Gegenteil; die Sensibilisierung für Pflichtthemen löst bei den meisten Mitarbeitenden wenig Begeisterung aus. Es benötigt ansprechende Schulungsmethoden, welche die Belegschaft zu einer ehrlichen Auseinandersetzung mit den Themen animieren. Die digitale Welt und ihre Möglichkeiten bieten hier die Chance, Schulungen unterhaltsam und mit dem nötigen Maß an Relevanz zu vermitteln das Vorhaben eines sicheren Unternehmens zu einem erfolgreichen und nachhaltigen Unternehmensprojekt heranreifen zu lassen. Doch die Voraussetzung dafür entspringt dem entsprechenden Engagement der höheren Unternehmensebene und ihrem konsequenten Einsatz für eine Kultur des Lernens und Verstehens.

3. Security Island: Von Einzelthemen zum Gesamtziel „Sicheres Unternehmen“

Die Risiken und Herausforderungen von heute werden im Unternehmen verschiedenen Thematiken zugeordnet und dementsprechend gehandhabt. Unterschiedliche Unternehmensabteilungen (z.B. die Abteilungen Compliance, Informationssicherheit, Arbeitsschutz usw.) agieren oft unabhängig voneinander. Dabei wird ein ähnliches Ziel verfolgt; die Stärkung der Sicherheit für Mitarbeitende, Führungskräfte und das Unternehmen selbst, damit Unternehmensziele verantwortungsvoll und erfolgreich verfolgt werden können.

Die digitale Schulungsplattform Security Island greift diese Herausforderung mit einer E-Learning Kursbibliothek auf, die digitale Kurse zu unterschiedlichsten Themen der Sicherheit umfasst. Diese soll als eine Sensibilisierungsmaßnahme unternehmensweit eingesetzt werden und Mitarbeitende in einem laufenden Prozess zu verschiedenen Themen schulen. Abseits der Risiken, die das Geschäftsfeld des Unternehmens betreffen und somit von Unternehmen zu Unternehmen und Branche zu Branche stark variieren können, werden bei Security Island die Themen so zusammengefasst, dass sie branchen- und marktunabhängig für Organisationen funktionieren. Denn selbst sicherheitsorientierte Unternehmen, bei denen der Aspekt der Sicherheit bereits fest im Geschäftsmodell verankert ist, müssen sich immer wieder neuen gesellschaftlichen, gesetzlichen und marktorientierten Anforderungen stellen. Dies greift Security Island mit folgender Idee auf:

„Zu der Unternehmenssicherheit von heute zählen sowohl die physische als auch mentale Sicherheit und Gesundheit der Mitarbeitenden. Dazu gehören Arbeitsschutz, Reisesicherheit, mentale Gesundheit, Resilienz aber auch das Wohlbefinden bedingt durch die Diversität und Inklusion. Daneben werden Themen aufgegriffen, die die Sicherheit im digitalen Raum betreffen, so z.B. die Informationssicherheit oder Cyber Security. Auch die Verantwortung für die Umwelt und das Umfeld des Unternehmens wird über Themen wie Corporate Social Responsibility, Nachhaltigkeit, Krisenmanagement, Fairness im Wettbewerb und im Betrieb umgesetzt. Hinzu kommt die Rechtssicherheit des Unternehmens und des täglich agierenden Mitarbeitenden. Diese wird in den Themen rund um die Compliance, den Datenschutz und das Arbeitsrecht abgebildet. Letztendlich wird das gesamte Themenportfolio vom Thema Leadership getragen, was die Basis jeder Organisation darstellt und ebenfalls als kontinuierliches Weiterbildungsthema den Führungskräften zur Verfügung stehen soll.“

Aufbauend auf dieser Idee wird Security Island zur unternehmensweiten Anlaufstelle, wenn es um die Sensibilisierung der Belegschaft zu Sicherheitsthemen geht. Unterschiedliche Abteilungen können so auf Security Island bedarfsorientiert zugreifen und ihre Schulungskampagne mit den E-Learning Kursen bereichern.

Um die Belegschaft trotz des breit gefächerten Themenpools und dem überschaubaren Interesse an vielen Pflichtthemen effektiv erreichen zu können, sind neben dem Einsatz digitaler Tools und der Ausarbeitung einer Schulungstrategie eine professionelle und unterhaltsame Ansprache der Mitarbeitenden nötig.

4. Ganzheitliche Awareness schaffen – die Kunst der digitalen Kommunikation

Zu einer Kultur des Lernens und Verstehens zum Zwecke der Unternehmenssicherheit gehört heute das digitale Lernen unablässig dazu. Das E-Learning gibt hierzu die Möglichkeit. Neben der Option, alle Mitarbeitenden mit einem entsprechenden Endgerät (Laptop, Smartphone, Desktop) thematisch zu erreichen, bietet das E-Learning eine Vereinfachung der Koordination von Terminen, Räumlichkeiten und digitalen Dokumentation für Schulungskampagnen. Insbesondere Unternehmen, die ihre Mitarbeitenden deutschlandweit oder international im Einsatz haben, profitieren von der flexiblen und kosteneffizienten Wissensvermittlung, bei der die Reisekosten für die Schulungsteilnehmenden wegfallen. Nicht umsonst erlebt das Thema E-Learning, gerade aktuell in Coronapandemie, einen starken Schub; dabei ist die Technologie und Idee sogar älter als das Internet selbst.

In den 90er und frühen 2000er Jahren waren E-Learnings meist kaum mehr als automatisierte Powerpoint-Präsentationen. Die fortgeschrittenen technologischen Möglichkeiten bieten im Jahr 2021 glücklicherweise ansprechende und nutzerfreundliche Formate. Ein E-Learning kann inzwischen problemlos auf den Einzelnutzer zugeschnitten werden und beispielsweise 4k Videos, Podcasts, Gamification Abschnitte, Interviews mit Experten, Quizzes und zahlreiche weitere Elemente enthalten. So kann nicht nur komplexes Wissen vermittelt, sondern auch jeder Lerntyp in einem Unternehmen angesprochen werden. Das Ziel: Lernen wird zu einem Erlebnis, aus “Education” wird “Edutainment”.

Ein weiterer wichtiger Aspekt ist die permanente Verfügbarkeit von Wissen im Unternehmen. Eine digitale Kursbibliothek ist immer und überall erreichbar, hat keine Öffnungszeiten und richtet sich gänzlich nach den Lernbedürfnissen aller Mitarbeitenden. Schulungen können beliebig oft und im eigenen Tempo wiederholt. Durch seine Niederschwelligkeit sprechen E-Learnings allen voran auch stillere Lerntypen an, die nicht gerne während eines Präsenzseminars öffentlich Fragen stellen, falls etwas unklar scheint.

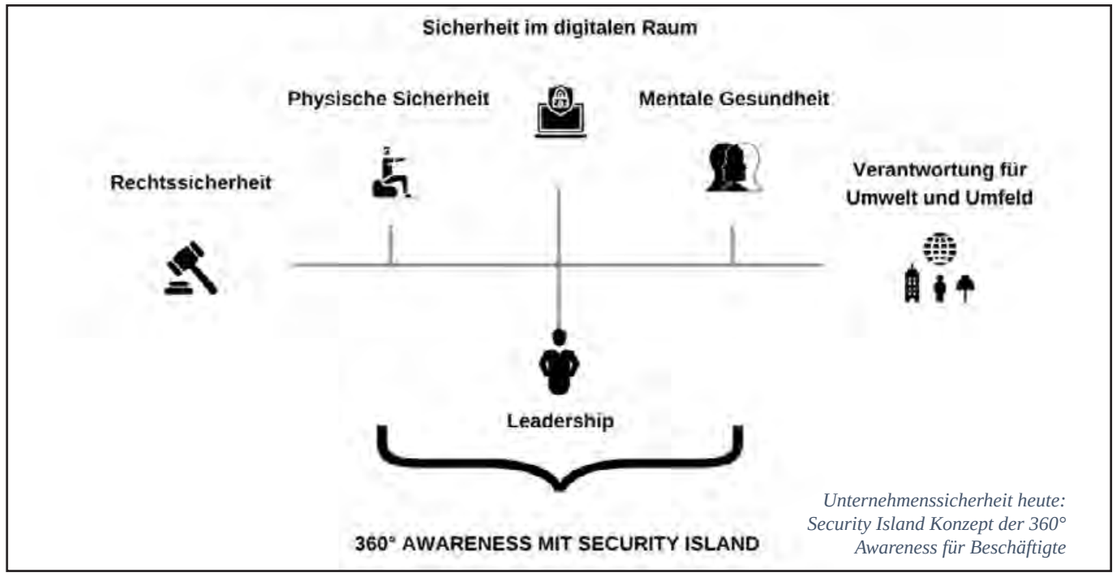
5. Die Grenzen von E-Learning

Bei allen augenscheinlichen Vorteilen haben digitale Lern- und Weiterbildungsangebote natürlich auch ihre Grenzen. “Eine häufige Fehlannahme, die uns immer wieder begegnet, ist, dass Unternehmen denken, E-Learnings würden Präsenzseminare, vertiefende Weiterbildungen und dergleichen komplett ersetzen”, sagt Uwe Röniger, Geschäftsführer des E-Learning-Herstellers mybreev (Security Island). “Das ist nicht der Fall.

Ein E-Learning kann sehr gut mit einem Fahrsicherheitstraining verglichen werden. Nach einem mehrstündigen Fahrsicherheitstraining ist kein Teilnehmender ein Profifahrer- oder Trainer. Jedoch hat der Teilnehmende Gefahrensituationen kennengelernt, weiß sie einzuordnen und kann entsprechend reagieren. Genauso verhält es sich mit E-Learnings, insbesondere im Cyber Security Segment. Das ist auch einer der Gründe warum z.B. Cyber Haftpflichtversicherungen häufig an das Angebot von E-Learning Anbietern gekoppelt sind bzw. günstigere Policen anbieten, wenn die Mitarbeitenden in einem Unternehmen regelmäßig E-Learnings zum Thema Cyber Security absolvieren.

E-Learnings können für Themen sensibilisieren, Interesse wecken, oder Wissen auffrischen. Tiefreichende Expertise erlangen Sie damit nicht – das ist aber auch gar nicht Sinn und Zweck von digitalen Lernangeboten. Eine aufeinander abgestimmte Kombination aus analogem und digitalem Lernen, sowie technische Lösungen sind nötig, um das Sicherheitskonzept von Unternehmen zu komplettieren.

Doch unabhängig von den vorhandenen digitalen Schulungsangeboten und Weiterbildungsmöglichkeiten in einem Unternehmen ist es unbedingt notwendig, dass das Thema Sicherheit – und damit verbunden das Wissen um die Sicherheit – im ganzen Unternehmen gelebt werden. Das obere Management mitsamt der Geschäftsführung befinden sich dabei in einer Vorbildfunktion, diese Themen zu kommunizieren und aktiv vorzuleben.



Unternehmenssicherheit heute: Security Island Konzept der 360° Awareness für Beschäftigte

CARE4AWARE

DAS SIND DIE GEWINNER 2020

Bereits anlässlich der ausgefallenen TAKE AWARE 2020 standen nach Voting durch unsere Jury die Care4Aware-Finalisten, aber auch die Sieger unserer drei Kategorien PROMOTE – PERFORM – CHANGE fest. Zur Erinnerung: Die Gewinner der drei Shortlists sollten am 17. März 2020 während des TAKE AWARE-Dinners in Stuttgart verkündet werden. Die Pandemie machte uns leider einen kurzfristigen Strich durch diese Rechnung. Und seit etwa anderthalb Jahren warten die Pokale und Urkunden auf eine Übergabe.

Dem bereiten wir nun ein Ende. Auf Grundlage der Abstimmung zwischen den Jury-Mitgliedern Dr. Katja Dörlemann (SWITCH/Schweiz), Michael Lardschneider (Munich Re), Nina Malchus (me – malchus eventmanagement), Wolfgang Reibenspies (FH Brandenburg, Ex-EnBW), Prof. Dr. Angela Sasse (RUB – Ruhr-Universität Bochum), Stefano Merenda und Ulrike Albanese (Propella Design) wurden im Rahmen eines, kurzen Online-Event die Awareness-Preise an Organisationen aus Deutschland, Österreich und der Schweiz verliehen,. die in den letzten Jahren durch vorbildliche Leistungen in Bezug auf Mitarbeiter-Sensibilisierung aufgefallen waren. Nominiert waren (s. a. ausführlicher Dokumentation im TAKE AWARE magazine #3):

Promote: Bestes Security Branding

1. Platz: IWC Schaffhausen

2. Platz: Bundesamt für Informatik und Telekommunikation (BIT)

3. Platz: AMAG Corporate Services AG

Perform: Beste (kurzfristige) Security Awareness-Kampagne

1. Platz Daimler AG

2. Platz: Fachhochschule St. Pölten GmbH

3. Platz: Hochschule Luzern

Change: Bestes (mittel- bis langfristiges) Security Awareness-Programm

1. Platz: Amadeus IT Group S. A.

2. Platz: Stadt Zürich

3. Platz: Daimler AG

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

MÄRZ 2021

KW	MO	DI	MI	DO	FR	SA	SO
09	1	2	3	4	5	6	7
10	8	9	10	11	12	13	14
11	15	16	17	18	19	20	21
12	22	23	24	25	26	27	28
13	29	30	31	1	2	3	4
14	5	6	7	8	9	10	11

- Fragen Sie die Identität Ihrer Gesprächspartner*innen ab – immer!
- Anrufende kennen keine Ansprechpartner*innen? Stellen aber Fragen zu Interna? Beenden Sie das Gespräch.
- Das Erwähnen von Namen (Kollegen, Geschäftsführung) ist kein Beleg für die Legitimität des Anrufenden.
- Diesbezügliche Auffälligkeiten melden Sie bitte an security@iwc.com

EXPECT IT. GUESS IT. WATCH IT.

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

Cyber Security Monat Oktober: Sie sind unser letztes Schutzschild

Gepostet von Maike Ring in Global Cyber Security (DE) am 01.10.2019 07:37:47

OFFIZIELL

Sowohl in Europa als auch in Amerika steht der Monat Oktober ganz im Zeichen der Sensibilisierung zu IT Sicherheit. Neben zahlreichen öffentlichen Veranstaltungen beteiligt sich auch Daimler mit einer weltweiten, internen Kampagne unter dem Motto „Die letzte Verteidigungslinie“ und lädt zum ersten, HACKtoberfest am 16. Oktober 2019.

Seit mehr als 130 Jahren gestalten wir Mobilität und haben ei
Auf dem Weg in eine digitale Zukunft gilt es dieses, neben Ki
Wenn unsere Spamfilter zu grob sind, eine Firewall zu niedrig
(DE) steht hierbei an Ihrer Seite!

Die letzte Verteidigungslinie

Wir geben Ihnen das Wissen rund um Sicherheit im Posteinga
in Ihrem Alltag. Wir weisen Sie auf die versteckten Gefahren
schützen können.

Schauen Sie sich direkt die erste Folge unserer Serie an, alle
Tag cybersecurity

Folgen
Teilen
Lesezeichen 14
Gefällt mir 83

AKTIONEN
Verwalten
Bearbeiten
Verschieben
Löschen

Kampagne unter dem Motto „Die letzte

Einladung zum HACKtoberfest 2019

In unserem Gewinnspiel „Game of Codes“ konnten Sie in den vergangenen Wochen bereits spielerisch Ihr Wissen herausfordern und erweitern. 198 Kolleginnen und Kollegen haben das richtige Lösungswort erraten und wir freuen uns die Gewinner bekannt zu geben. Eine Eintrittskarte für die Global Cyber Security Convention 2020 haben gewonnen. Herzlichen Glückwunsch!

Aber Sie alle haben gewonnen, denn wir laden zum ersten, internationalen Cyber Security Tag, dem HACKtoberfest, am 16. Oktober 2019 an Ihrem Standort ein. Weltweit haben Ihre lokalen Information Security Officer ein spannendes und abwechslungsreiches Programm vorbereitet. Lernen Sie Ihr lokales Cyber Security Team kennen, besuchen Sie interessante Vorträge und erfahren Sie mehr zum Thema an den lokalen Marktständen.

Neugierig? Folgen Sie unserer Global Cyber Security Day 2020 Community im Social Intranet und teilen Sie Ihre Erlebnisse an diesem Tag. Durch Ihre Diskussionen, Beiträge und Fotos zeigen Sie, dass wir Seite an Seite weltweit die beste Verteidigung gegen Cyber Kriminelle bilden.

Wir freuen uns auf Sie!

Weitergehende Informationen über Cyber Security finden Sie auf Global Cyber Security (DE). Für spezifische Fragen stehen wir gerne unter cyber.security@daimler.com zur Verfügung.

Daimler
Global Cyber Security

Wir danken an dieser Stelle bereits jetzt unseren beiden Schauspielern Kristina Rose und Philipp Hühler.

September 2019
August 2019
Juli 2019
Juni 2019
Mai 2019
April 2019
März 2019
Februar 2019
Januar 2019
Dezember 2018

Nach Tag:
cyber security
cybersecuri

AKTUELLE EINTRÄGE

Daimler AG

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

Introduction

IT’S UP TO YOU

Are we secure?

48,000 TRAVEL AGENTS RELY ON US TO GO FURTHER

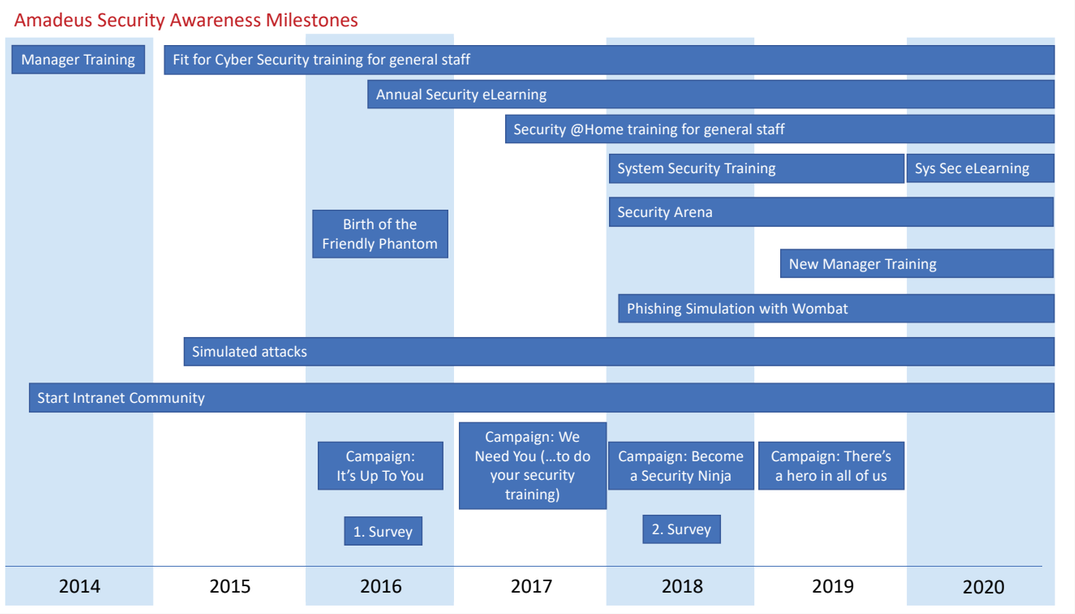
Posters, screensavers and office signage

Dear Everyone

We are launching an important group-wide initiative to ensure that we fulfil our care of duty to look after sensitive data, and in so doing look after our reputation.

These guidelines provide an overview of the CyberSecurity campaign being launched across the business to all employees. It provides the simple principles that will enable all materials to reflect and reinforce the key messages in a consistent and coherent way.

These are basic guidelines, which do not cover the range of applications that we might need. As such they require you to interpret and apply the principles with common sense. For assets and guidance, please contact xxx.



NIEMAND IST ANONYM – TÄTER ANHAND IHRER SPRACHE IDENTIFIZIEREN

EIN MEDIAL BEKANNT GEWORDENER FALL

von Steffen Hessler

Am Abend des 11. April 2017 explodieren während der Fahrt drei in einer Hecke versteckte Sprengsätze in direkter Nähe zum Bus der Fußballmannschaft von Borussia Dortmund. Am Anfang der Ermittlungen tauchen sowohl islamistische als auch linksextremistische Bekennerschreiben auf. Die Schreiben werden u. a. auch von forensisch-linguistischen Expert/inn/en analysiert und auf ihre Authentizität hin geprüft. Handelt es sich um einen islamistisch motivierten Terrorakt, um eine Tat aus dem linksextremistischen Milieu oder hatte das Bombenattentat einen ganz anderen Hintergrund?

Im Laufe der Ermittlungen stellt sich heraus, dass die Echtheit der Bekennerschreiben stark bezweifelt werden kann.[1] [2] Vielmehr ist es so, dass der später Verurteilte Verkaufsoptionsscheine auf die Aktie von Borussia Dortmund gekauft hatte und keine politisch oder religiös motivierten Gründe für den Anschlag vorlagen.[3] Es handelt sich also um eine Tat, die ausschließlich Profit durch Kursmanipulation zum Ziel hatte.

In diesem Fall konnten forensisch-linguistische Analysen helfen, bestimmte Gruppen als potentielle Schreiber/innen der Erpresserbriefe auszuschließen und den infrage kommenden Täterkreis einzugrenzen.

Erpressungen als Alltagsphänomen

Jeder hat das schon einmal mitbekommen, wenn er/sie im Supermarkt einkaufen geht: Schokolade X, Pudding Y oder Käse Z werden zurückgerufen. Die Gründe hierfür können verschiedene sein. Im Internet oder in Regionalzeitungen liest man sehr häufig über solche Rückrufaktionen.[4] Es besteht z. B. die Gefahr, dass kleine Metallteile o. ä. in den Produkten enthalten sein können. Doch was ist die Ursache für diese Gefahren? Vielleicht kam es zu Fehlern im Betriebsablauf. Solche Probleme sind ärgerlich und gefährlich, aber nicht vollständig auszuschließen. Vielfach kann die Ursache für Produktrückrufe jedoch auch darin liegen, dass ein Betrieb erpresst wird. In diesem Fall werden Produkte absichtlich verunreinigt und der Betrieb wird unter Druck gesetzt. In solchen Fällen liegen oft Erpresserschreiben vor. Diese können sowohl von Außenstehenden als auch von so genannten Innentätern stammen, also Leuten, die direkt mit einem Unternehmen zu tun haben, vielleicht dort beschäftigt sind oder waren.

Doch nicht nur der Lebensmitteleinzelhandel ist von Erpressungen betroffen. Erpressungen und Drohungen gegen und innerhalb von Unternehmen sind zu einem Alltagsphänomen geworden. In vielen Fällen werden diese Komplikationen gar nicht publik. Die Angst vor Imageverlust und davor, dass die Probleme sich noch weiter verschlimmern oder weitere hinzutreten, ist zu groß.

In solchen Fällen kann eine Autorschaftsanalyse im Rahmen einer forensisch-linguistischen Untersuchung helfen. Autorschaftsanalysen können Hinweise darauf geben, wer den Erpresserbrief geschrieben hat.

1 https://www.faz.net/aktuell/politik/inland/erhebliche-zweifel-an-islamistischem-bvb-bekennerschreiben-14972750.html Letzter Zugriff am 13.09.2021
2 https://www.sueddeutsche.de/medien/anschlag-in-dortmund-raetsel-um-zweites-dortmund-schreiben-1.3462094 Letzter Zugriff am 13.09.2021
3 https://www.spiegel.de/panorama/justiz/borussia-dortmund-ermittler-fassen-mutmasslichen-bvb-bomber-a-1143998.html Letzter Zugriff am 13.09.2021
4 https://www.ruhr24.de/service/rueckruf-edeka-wurst-aktuell-lebensmittel-verletzung-heute-warnung-neu-deutschland-90317454.html Letzter Zugriff am 13.09.2021

Die Erpressung einer Supermarktkette oder eines Lebensmittelproduzenten ist ein Thema, das medial recht präsent ist. Forensisch-linguistische Analysen können allerdings in vielen verschiedenen Bereichen dazu beitragen, Schreiber/innen anhand ihrer Schreibstile zu identifizieren. Autorenerkennung wird für Unternehmen u. a. auch in den folgenden Bereichen eingesetzt:

- Mobbing,
- interne Beleidigung,
- üble Nachrede und Verleumdung (§§ 185ff StGB),
- falsche Anschuldigung (§ 164 StGB),
- Bedrohung (§ 241 StGB),
- öffentliche Verleumdung und Bedrohung (§§ 187 und 188 Abs. 2 StGB),
- Verrat von Betriebsgeheimnissen (§ 120 Betriebsverfassungsgesetz)
- oder Werks- bzw. Wirtschaftsspionage.

Diese Liste ist keineswegs erschöpfend. Sie gibt allerdings schon einen guten Eindruck, wie vielfältig linguistische Analysen bei der Tätersuche etc. eingesetzt werden können.

Dem Täter auf der Spur – Textvergleiche

Doch wie funktioniert das Ganze überhaupt? Jede/r Schreiber/in verfügt über einen relativ spezifischen Schreibstil, macht u. U. bestimmte Fehler und verwendet wiedererkennbare Stilmerkmale. Sollte also ein Text vorliegen, der forensisch-linguistisch untersucht werden soll, kann dieses fragliche Schreiben mit anderen Texten von infrage kommenden Schreiber/inne/n verglichen werden. Diese Schreiben bezeichnet man als Vergleichstexte. Bei Textvergleichen werden verschiedene sprachliche Ebenen berücksichtigt. So bestehen Texte nicht bloß aus einer Reihe von aufeinander folgenden Wörtern.

Bei der Analyse können z. B. grammatische Formen (Morphologie), Bezüge verschiedener Textelemente zueinander (Syntax) und die Zeichensetzung (Interpunktion) wichtige Indikatoren für einen relativ individuellen Schreibstil beinhalten. Natürlich spielt auch die Verwendung bestimmter Wörter (Lexik) und ihrer Bedeutung (Semantik) mit einer bestimmten Gebrauchsintention (Pragmatik) eine Rolle.

Anhand der im Textvergleich gefundenen Übereinstimmungen und Unterschiede kann ein Wahrscheinlichkeitsgrad abgeleitet werden, ob zwei oder mehr Texte von der/dem gleichen Autor/in stammen.

Die Skala der Übereinstimmung reicht von „mit an Sicherheit grenzender Wahrscheinlichkeit“ bis „non liquet“ (kann nicht entschieden werden). Diese Skala wird ebenfalls von der Autorenerkennung des Bundeskriminalamts verwendet.

1. mit an Sicherheit grenzender Wahrscheinlichkeit
2. mit sehr hoher Wahrscheinlichkeit
3. mit überwiegender Wahrscheinlichkeit
4. mit leicht überwiegender Wahrscheinlichkeit
5. wahrscheinlich
6. non liquet (kann nicht entschieden werden)

Tätersuche anhand von Metadaten – Textanalysen ohne Vergleichsmaterial

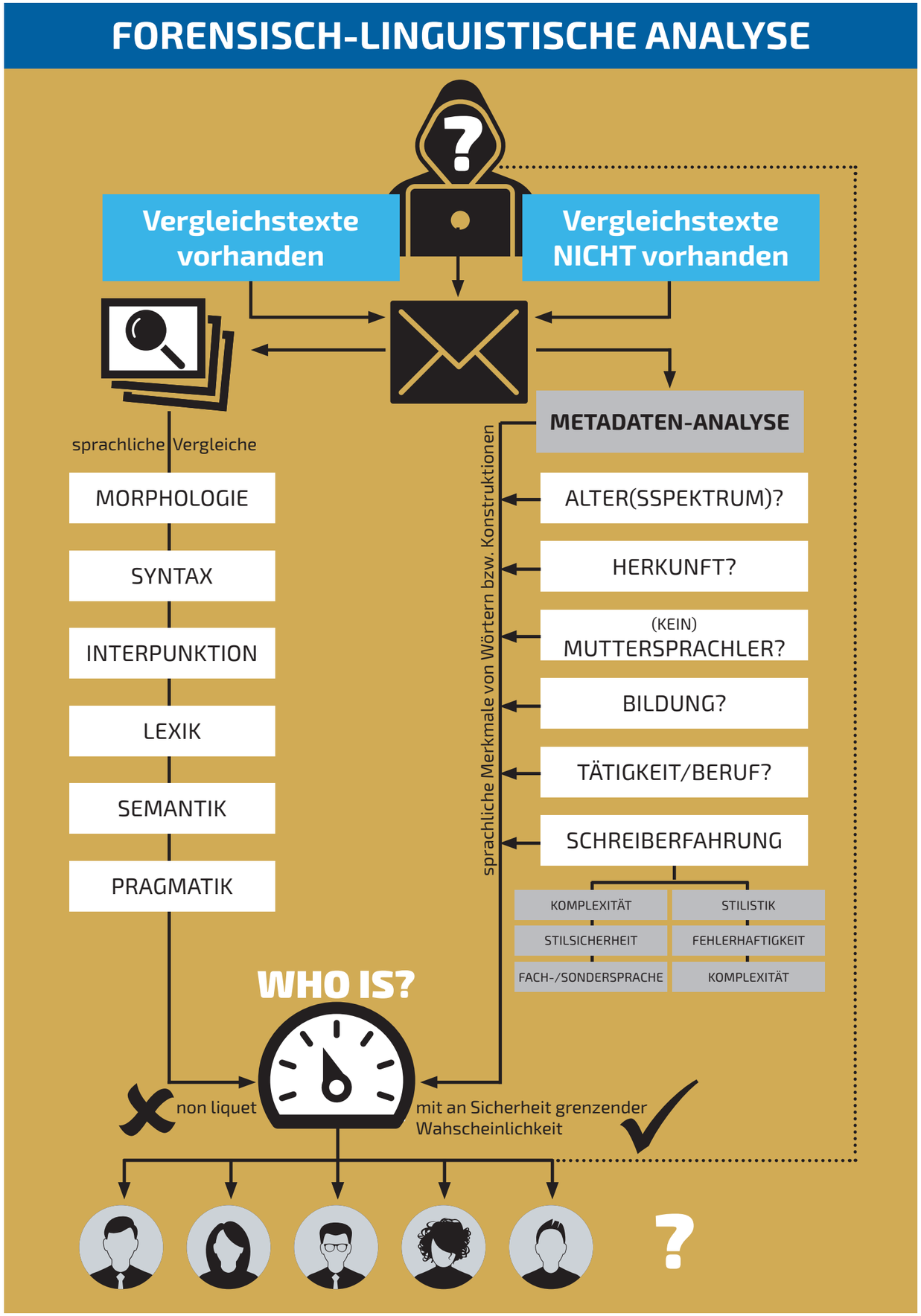
Eine gänzlich andere Herausforderung stellt sich, wenn es keine Vergleichstexte gibt. In diesem Fall wird eine Textanalyse durchgeführt. Auch hierbei wird ein Text, beispielsweise eine Erpressung, auf allen Ebenen der Sprachbetrachtung analysiert. Anhand der gefundenen Merkmale lassen sich Aussagen zu den Metadaten der/des Autorin/Autors treffen. Die Verwendung bestimmter Wörter oder Konstruktionen gibt Hinweise auf das ungefähre Alter bzw. ein Altersspektrum, in dem die/der Schreiber/in zu verorten ist.

Verschiedene sprachliche Merkmale können Fingerzeige für die Herkunft sein. Das betrifft z. B., ob diejenige/derjenige, die/der schreibt, Muttersprachler/in ist, oder nicht. Außerdem geben Texte Hinweise auf die regionale Herkunft bzw. die Region der sprachlichen Sozialisation. Ist die Autorin im Süden Deutschlands aufgewachsen oder kommt der Autor aus dem Norden? Werden sprachliche Merkmale verwendet, die in Österreich oder der Schweiz üblich sind? Forensisch-linguistische Textanalysen geben hier Aufschluss und die regionalen Bereiche können mithilfe von Sprachatlanten bzw. Sprachkarten weiter eingegrenzt werden. Weitere Bereiche, zu denen sich Aussagen treffen lassen, sind beispielsweise Bildung, Tätigkeit und Beruf. Ein wichtiger Indikator ist hier die Schreiberfahrung bzw. Geübtheit bei der Erstellung von Texten bestimmter Textsorten anhand der Komplexität, der Stilistik bzw. Stilsicherheit sowie Fehlerhaftigkeit, die analysiert werden können. Das Vorhandensein der Verwendung von Merkmalen von Fach- bzw. Sondersprachen präzisiert das Autorschaftsprofil bzw. grenzt den Kreis infrage kommender Schreiber/innen weiter ein.

Die/Der Schreiber/in erscheint durch abgeleitete Metadaten als Repräsentant/in einer bestimmten Personengruppe. Im Rahmen der forensisch-linguistischen Analyse von in krimineller Absicht verfasster Schreiben besteht das Ziel, den Kreis der Autorschaft bzw. den Täterkreis einzugrenzen.

Schutz für Unternehmen

Doch was bedeutet das konkret? In Ihrem Unternehmen taucht ein Text auf, der Mitarbeiter/innen oder das Unternehmen gefährdet bzw. bedroht oder Betriebsabläufe stört. Dann können forensisch-linguistische Analysemethoden helfen, die Urheber/innen des Schreibens zu ermitteln. Es wird untersucht, aus welcher Richtung das Schreiben kommen könnte. Ist die Herkunft eher von außen oder von innen anzunehmen? Wenn der Täterkreis bereits eingegrenzt werden kann, wird geprüft, ob Vergleichsschreiben vorliegen. Falls ja, können Textvergleiche durchgeführt werden. Grundsätzlich können Textanalysen angestellt werden, um die Metadaten der/des Autorin/Autors einzugrenzen. So können Verdachtssituationen bestärkt oder entkräftigt werden.

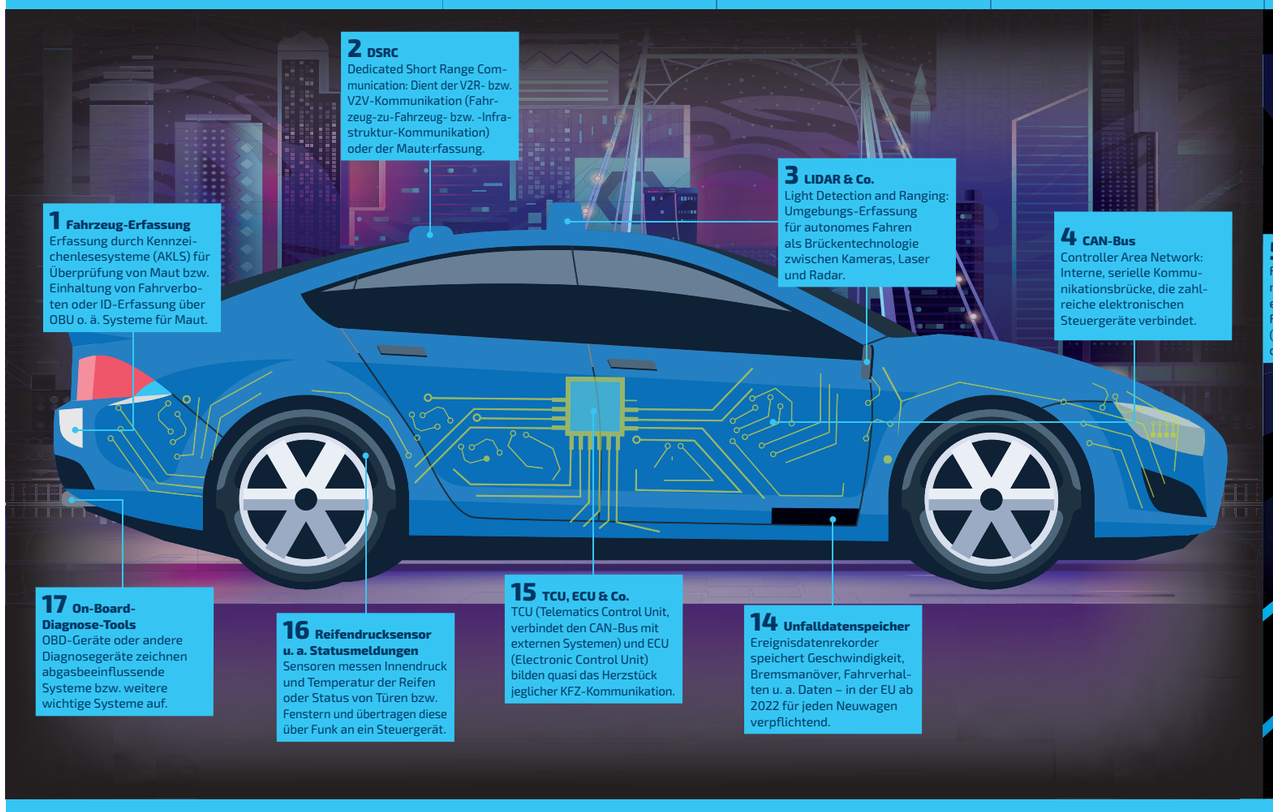


Halb Auto – halb Computer: Würde das „TAKE AWARE sec&life magazine“ als Printausgabe erscheinen oder „Bravo“ heißen, wäre das hier abgebildete Spielfeld der neuen „Security Arena“-Station „Connected Car“ unser Miniposter zum Rausnehmen. Ohne Printausgabe ist dies ein Wimmelbild zum Entdecken. Da E-Mobilität endlich an Fahrt gewinnt, ist auch die zunehmende Bedeutung der Kollateralthemen „Infosec“ und „Datenschutz“ nicht mehr von der Hand zu weisen. Die Station „Connected Car“ ist im Übrigen im eigenen Branding via known_sense lizenzierbar.

DATENEMPFÄNGER

- **FAHRZEUG-HERSTELLER/-WERSTATT**
- **SATELLIT**
- **NOTRUFSYSTEM**
- **MAUTSTELLE**
- **V2V – CAR-TO-CAR COMMUNICATION**
- **C2I/V2R** (CAR-TO-INFRASTRUCTURE/ VEHICLE-TO-ROADSIDE)
- **VERSICHERUNG**
- **ANDERE**

Prüfstelle
Diverse Clouds
Vermieter & Sharing-Anbieter
Verkehrszentrale & Co.
Mitfahrer
etc.



1 Fahrzeug-Erfassung
Erfassung durch Kennzeichenlesesysteme (AKLS) für Überprüfung von Maut bzw. Einhaltung von Fahrverboten oder ID-Erfassung über OBU o. ä. Systeme für Maut.

2 DSRC
Dedicated Short Range Communication: Dient der V2R- bzw. V2V-Kommunikation (Fahrzeug-zu-Fahrzeug- bzw. -Infrastruktur-Kommunikation) oder der Mauterfassung.

3 LIDAR & Co.
Light Detection and Ranging: Umgebungs-Erfassung für autonomes Fahren als Brückentechnologie zwischen Kameras, Laser und Radar.

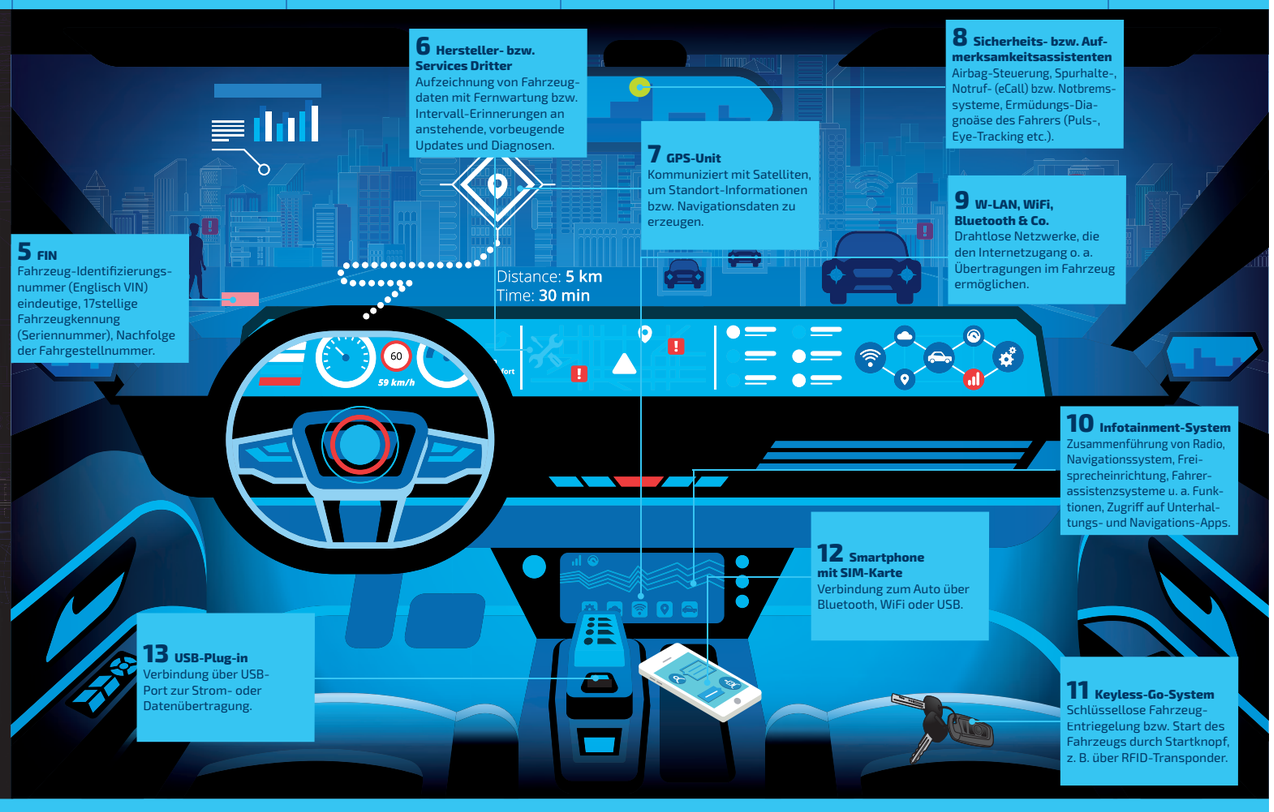
4 CAN-Bus
Controller Area Network: Interne, serielle Kommunikationsbrücke, die zahlreiche elektronischen Steuergeräte verbindet.

17 On-Board-Diagnose-Tools
OBD-Geräte oder andere Diagnosegeräte zeichnen abgasbeeinflussende Systeme bzw. weitere wichtige Systeme auf.

16 Reifendrucksensor u. a. Statusmeldungen
Sensoren messen Innendruck und Temperatur der Reifen oder Status von Türen bzw. Fenstern und übertragen diese über Funk an ein Steuergerät.

15 TCU, ECU & Co.
TCU (Telematics Control Unit, verbindet den CAN-Bus mit externen Systemen) und ECU (Electronic Control Unit) bilden quasi das Herzstück jeglicher KFZ-Kommunikation.

14 Unfalldatenspeicher
Ereignisdatenrekorder speichert Geschwindigkeit, Bremsmanöver, Fahrverhalten u. a. Daten – in der EU ab 2022 für jeden Neuwagen verpflichtend.



6 Hersteller- bzw. Services Dritter
Aufzeichnung von Fahrzeugdaten mit Fernwartung bzw. Intervall-Erinnerungen an anstehende, vorbeugende Updates und Diagnosen.

5 FIN
Fahrzeug-Identifizierungsnummer (Englisch VIN) eindeutige, 17stellige Fahrzeugkennung (Seriennummer), Nachfolge der Fahrgestellnummer.

7 GPS-Unit
Kommuniziert mit Satelliten, um Standort-Informationen bzw. Navigationsdaten zu erzeugen.

8 Sicherheits- bzw. Aufmerksamkeitsassistenten
Airbag-Steuerung, Spurhalte-, Notruf- (eCall) bzw. Notbremssysteme, Ermüdungs-Diagnoäse des Fahrers (Puls-, Eye-Tracking etc.).

9 W-LAN, WiFi, Bluetooth & Co.
Drahtlose Netzwerke, die den Internetzugang o. a. Übertragungen im Fahrzeug ermöglichen.

10 Infotainment-System
Zusammenführung von Radio, Navigationssystem, Freisprecheinrichtung, Fahrerassistenzsysteme u. a. Funktionen, Zugriff auf Unterhaltungs- und Navigations-Apps.

12 Smartphone mit SIM-Karte
Verbindung zum Auto über Bluetooth, WiFi oder USB.

13 USB-Plug-in
Verbindung über USB-Port zur Strom- oder Datenübertragung.

11 Keyless-Go-System
Schlüssellose Fahrzeug-Entriegelung bzw. Start des Fahrzeugs durch Startknopf, z. B. über RFID-Transponder.

SECURITY ARENA:
CONNECTED CAR SECURITY

WER DU BIST! WAS DU KONSUMIERST! WO DU WARST! WEN DU KENNST! WIE WIE DU FÄHRST! WIE ES DEINEM AUTO GEHT!

known_sense
awareness you can touch.

»BIEDERMEIER« ODER »ICH WILL HIER RAUS?«

GOOD COVID-PRACTICE: WIE KOMMEN WIR MIT HALBER SENSIBILISIERUNG DURCH DIE KRISE?

CORONA-UMFRAGE

KOMPILIERT UND MIT EINER EINLEITUNG VON DIETMAR POKOYSKI

Am 16. März 2020 wird der erste Lockdown im Rahmen der Corona-Pandemie beschlossen. Am selben Abend wollen etwa 60 Gäste – das sind ungefähr die Hälfte der TAKE AWARE-Konferenzanmeldungen 2020 – in einer Stuttgarter Craft Beer-Bar zum Meet & Greet zusammenkommen, um in lockerer Atmosphäre über das Thema Security Awareness zu sprechen. Zu diesem Zeitpunkt ist die 4. TAKE AWARE/SEXY SECURITY-Doppelkonferenz, die im Innenministerium Baden-Württemberg geplant war, jedoch längst abgesagt, obwohl nur wenige Tage zuvor der damalige Fußball-Zweitligist VFB Stuttgart im Gottlieb-Daimler-Stadion vor knapp 50.000 Zuschauern gegen Arminia Bielefeld spielte.

Awareness ohne Präsenz und echte Beziehungen?

In den Monaten danach folgten bis heute mehrere Lockdowns und für die interne Kommunikation in den Unternehmen eine Phase der Digitalisierung mit einem harten Beziehungsentzug – zumindest was den Face-to-face-Kontakt angeht, der ja für unsere Community so wichtig zu sein scheint, wenn man auf den hohen Anteil von Präsenzformaten in den Sensibilisierungskampagnen schaut.

Und bekanntlich führen ja aktuell auch die meisten Umfragen unter Mitarbeitenden zu der Erkenntnis, dass das Büro unter den allermeisten gerade als sozialer Schmelztiegel vermisst wird. Das Erleben im eigenen Homeoffice wird dann oft als „nichts Halbes und nichts Ganzes“ beschrieben.

Davon abgrenzend existiert aber offensichtlich ein weiteres Phänomen innerhalb einer Art Zweiteilung, wie der Psychologe Stephan Grünewald von rheingold mithilfe zahlreicher Tiefeninterviews für Corona-Studien evaluiert hat.

Grünewald sagt: „Die eine Hälfte erlebt Corona als existentielle Verunsicherung, als Zeit der Enge und Überforderung. Die andere Hälfte hatte eine schöne Zeit in den vergangenen Monaten. Die haben aufgeräumt, viel gelesen, hatten Zeit für sich. Da hat sich eine Art Corona-Biedermeier etabliert. Viele hofften sogar insgeheim, dass die Zeit der Entschleunigung noch lange weitergehen könnte. Das sind vor allem Rentner, Beamte, Menschen, die sich keine Sorgen machen müssen. Diese Spaltung war bereits vor Corona da, aber sie durch die große Solidarität in der ersten Phase überdeckt worden. Jetzt tritt sie umso heftiger zutage.“

Corona-Biedermeier?

Aber was ist davon in den aktuellen-Awareness-Maßnahmen spürbar? Da zahlreiche Konferenzbesucher zu den Kunden von known_sense bzw. mybreev gehören, standen wir in einem regelmäßigen Austausch mit der Awareness-Community und hörten interessiert zu, wie sich die Dinge in den Unternehmen entwickelten.

Ende 2020 verschickten wir einen Fragebogen mit insgesamt 5 Fragenkomplexen, die uns besonders interessierten, um das Ohr am Puls unserer Community zu halten und anderen aus dieser Community zu präsentieren, wie Dritte mit dem Thema während der Pandemie umgehen.

Heute – anderthalb Jahre nach dem ersten Lockdown und mehr als ein halbes Jahr nach dem Start der Umfrage – publizieren wir die interessanten Antworten im Rahmen eines tabellarischen Vergleichs von 5 sehr unterschiedlichen Organisationen aus Deutschland und aus der Schweiz, garniert um ein weiteres Interview mit einer Projektmanagerin, die dem Thema Security Awareness ebenfalls seit Jahren als Freelancerin verbunden ist.

Immerhin hat eines der hier interviewten Unternehmen, die Commerzbank, 2020 für Ihre internationale Awareness-Kampagne „Hacker Island“ den „Outstanding Security Performance Award“ (OSPA) in der Kategorie „Herausragende Security-Trainings-Initiative“ gewonnen (siehe Screenshot der Online-Verleihung links unten). Die Kampagne wurde vor Corona geplant und quasi parallel zum ersten Lockdown im Marz 2020 unter Pandemiebedingungen gelauncht.

Wir hoffen, dass Sie sich als Leser/in – sofern Sie ebenfalls für Awareness in Ihrem Unternehmen zuständig sein sollten – in vielen Antworten wiedererkennen und dennoch einen Take Away generieren, eine Art Anregung für die nächsten Monate oder sogar darüber hinaus.

Die Interviewabfragen fanden schriftlich zwischen Dezember 2020 und April 2021 statt. Wir bedanken uns bei allen Teilnehmenden, die wir in den Interviews duzen, für ihre freundliche Mitarbeit an diesem qualitativen Benchmark.

CORONA-UMFRAGE (1/4)

Unternehmen	Amadeus IT Group	Commerzbank AG	IWC Schaffhausen	RWE AG	SWITCH
Interviewpartner/in **Fragen**	Thomas Wepner, Senior Corporate Security Officer	Michael Peters, Information Security Awareness Spezialist bei Group Risk Management | Cyber Risk & Information Security	Sascha Maier, Head of IT & Cyber Resilience	Fabian Cholewa, Information Security Officer und Awareness & Cyber Security Manager, Konzernsicherheit | Group Security | Cyber Security	Katja Dörlemann, Awareness-Spezialistin und Cornelia Puhze, Communication Managerin
Frage 1: Wie geht es dir? Was hat sich m Laufe der Pandemie in deinem Job geändert? Haben sich infolge von Corona z. B. Beziehungen innerhalb deines Teams oder mit Vorgesetzten auffällig verändert?	Die Beziehungen innerhalb unseres Teams und zu unseren Vorgesetzten haben sich meines Erachtens sogar verbessert. Das Bewusstsein für die schwierige Lage des Unternehmens und der Kollegen hat zu intensiveren persönlichen Gesprächen geführt und den Zusammenhalt innerhalb des Teams gestärkt.	Der Homeoffice-Anteil hat sich naturgemäß deutlich erhöht. Natürlich fehlt hie und da der spontane informelle Austausch mit Kollegen und Vorgesetzten beim Kaffee oder „zwischen Tür und Angel“. Wir haben versucht, dies durch einen regelmäßigen „Morning Video Call“ zu ersetzen, das funktioniert auch recht gut. Wirklich gravierende Auswirkungen auf die Zusammenarbeit o. ä. sind aber nicht festzustellen.	Dank der guten Kommunikation von Geschäftsleitung und Krisenteam waren wir der Krise immer einen Schritt voraus, was bei den Kollegen und Kolleginnen durchaus Vertrauen gebildet hat. Die Führungskräfte haben sich entsprechend angepasst und wurden durch HR permanent unterstützt.	Ich bin bisher gut durch die Pandemie gekommen. Dafür bin ich dankbar. Unser Team ist stark gewachsen, was mich wirklich freut. Jedoch gibt es manche Neue, die bereits seit Monaten dabei sind und sich aufgrund von Corona noch nicht persönlich kennengelernt haben. Aber jetzt kommt das Gute: Es funktioniert trotzdem! Das spricht für eine positive Veränderung in unserem Konzern – wir werden digitaler. Nicht nur die technischen Möglichkeiten müssen dafür bereitgestellt werden, es müssen sich auch alle darauf einlassen: Von Führungskräften, die ihre Mitarbeitenden nicht mehr täglich um sich haben, bis hin zu denjenigen, die jetzt selbstständiger arbeiten und mit neuen Herausforderungen konfrontiert sind. Der Unterschied zur Zeit vor Corona: Vieles muss digital realisiert werden – sonst stoppt das Business.	Der Austausch mit den Teamkollegen und -kolleginnen ist etwas schwieriger geworden. Dedizierte Austausch-Meetings helfen für die nötigsten Informationen, aber das allgemeine „Was machst Du gerade so?“ fällt im Homeoffice weg. Gerade für neu zu uns gestoßene Kollegen und Kolleginnen ist es etwas schwierig, sich ins gesamte Team zu integrieren.
Frage 2: Vor welchen besonderen Herausforderungen steht die Security Awareness derzeit in deinem Unternehmen? Wie unterscheiden diese sich zu denen vor März 2020?	Die erste Herausforderung ist die enorm gestiegene Zahl der Angriffsversuche auf Menschen (Phishing, Social Engineering) und die schamlose Ausnutzung der pandemiebedingten Ängste und Unsicherheiten, zum Beispiel in Form von Corona-basierten Phishingmails. Die zweite Herausforderung ist die höhere Schwierigkeit, unsere Kollegen mit unseren Botschaften zu erreichen. Lokale Face-to-face Security Awareness-Aktivitäten wie Präsenztrainings und Security-Events sind seit Anfang März durch Reisebeschränkungen und Homeoffice unmöglich. Außerdem entfallen sämtliche lokalen Marketingkanäle wie z. B. Poster, TV-Screens etc., da unsere Mitarbeiter überwiegend im Homeoffice arbeiten müssen. Für Kommunikationsmaßnahmen bleiben nur noch E-Mail und Intranet. Bei beiden stehen wir in noch größerer Konkurrenz zu anderen wichtigen Themen als sonst.	Es handelt sich hierbei um eine Gratwanderung: Einerseits ist es eine große Herausforderung, möglichst viele Menschen mit den Themen zur Informationssicherheit zu erreichen. Die tägliche Informationsflut – gepaart mit immer weniger Zeit der Mitarbeiter, sich dieser zu widmen – macht es schwieriger, die Themen bei den Mitarbeitern wirksam zu platzieren.Andererseits darf man den Bogen hinsichtlich der Menge und Frequenz der Veröffentlichungen zur Informationssicherheit (Pflicht Web Based Trainings, Online Formate der Kampagne, Präsenzformate etc.) auch nicht überspannen, damit Mitarbeiter diese wichtigen Themen nicht ausschließlich als weiteren Anteil der ohnehin zu großen Informationsflut identifizieren (und damit evtl. inhaltlich nicht wirklich wahrnehmen).	Dank der bereits bestehenden Awareness konnten wir das ganze gut abfangen und mussten uns keine großen Sorgen machen bzw. neue Maßnahmen ergreifen. Das sieht im Moment auch nicht anders aus. Wir hatten Mitte November 2020 einen „ungewollten“ Phishing Test (Fehlkonfiguration eines neues Tools). Alle Mitarbeitenden haben eine verlockende Mail erhalten. Über 95% haben nicht draufgeklickt. 50% haben es gemeldet. Daher alles gut.	Ich sehe das mobile Arbeiten als eine der größten Herausforderungen. Denn hier vermengt sich die Sicht der Privatperson mit der Sicht des Arbeitnehmenden. Ein Beispiel: Wenn es für mich als Privatperson selbstverständlich ist, dass ein kostenloser Clouddienst für den Austausch einer Datei verwendet wird, ist das aus Businesssicht nicht die beste Wahl. Denn dort können sensible Informationen ungewollt ihre Vertraulichkeit verlieren. Und das ist aus meiner Sicht die große Herausforderung: Sich und sein Handeln hinsichtlich der Security in den eignen vier (und eigentlich gefühlt sicheren) Wänden zu reflektieren.	Homeoffice! Die Mitarbeitenden sind nicht mehr am Platz, tauschen sich nicht mehr jeden Tag aus und laufen auch nicht an Postern vorbei. Gleichzeitig hat sich das Arbeits- und somit auch Bedrohungsumfeld der Mitarbeitenden verändert. Es müssen nun bestimmte Regeln mit Nachdruck kommuniziert werden: VPN nutzen, Umgang mit sensitiven Informationen zu Hause, Support im Homeoffice etc.

CORONA-UMFRAGE (2/4)

Unternehmen	Amadeus IT Group	Commerzbank AG
Frage 3: Welche Security Awareness-Maßnahmen wurden in den letzten Monaten in deinem Unternehmen durchgeführt und wie unterscheiden die sich zu denen im Vorjahr bzw. denen im Januar/Februar 2020? D. h. welche ursprünglich geplanten Maßnahmen wurden ggf. NICHT durchgeführt, sind verschoben oder abgesagt worden – mit welchen Eindrücken/Ergebnissen?	Die erste Auswirkung der Pandemie war die Absage eines mehrtägigen Train-the-Trainer Workshops. Ursprünglich wollten wir unsere sehr erfolgreichen Präsenztrainings und Events wie die „Security Arena“ schneller in unsere Standorte auf allen Kontinenten bringen. Auch bereits geplante lokale Events an mehreren Standorten mussten abgesagt werden. Zu Beginn der Pandemie waren wir fast ausschließlich mit Kommunikationsmaßnahmen beschäftigt, um der Flut von Corona-basierten Angriffsversuchen möglichst viel Aufklärung entgegen zu setzen. Auch die Umsetzung verschärfter Sicherheitsmaßnahmen musste schnell und klar kommuniziert werden. Im nächsten Schritt haben wir uns überlegt, wie wir bereits laufende Trainingsprogramme für besonders kritische Zielgruppen ohne die Möglichkeit von Präsenztrainings weiterführen könnten. Die Lösung bestand aus zwei verschiedenen Ansätzen. Ein bisher lokal durchgeführtes Ganztagestraining für Systemadministratoren etc. wurde komplett in ein SCORM-basiertes Onlinetraining mit Übungs-Lab in der Cloud umgewandelt. Ein ebenfalls bisher lokal durchgeführtes Training für sämtliche Manager mit Personalverantwortung wurde in ein live durchgeführtes Online Training umgewandelt. Überraschenderweise war auch die Teilnahme an unserem jährlichen Online Security Training für alle Mitarbeiter höher als jemals zuvor.	Wir konnten unsere neue Informationssicherheitskampagne planmäßig im März 2020 starten – jedoch ausschließlich das „Online“-Format, d. h., die 14tägige Veröffentlichung einer Episode unseres „Hacker Island“ Zyklus (bestehend aus einem humorvollen Comic, Goldenen Regeln und einem sachlich geschriebenen Artikel). Die Veröffentlichungen haben wir während der gesamten Zeit beibehalten und führten diese bis März 2021 fort. Dann endete planmäßig nach 24 Folgen die in unseren Veröffentlichungen erzählte Geschichte von Käpt’n Safe und seinem Papagei Easy. Inzwischen ist bereits Staffel 2 mit 12 neuen Folgen gestartet. Eine spätere Fortsetzung ist nicht ausgeschlossen. Die ursprünglich geplanten Präsenzformate (Security Messe, Rollout Spielformat Security Arena) mussten zuletzt leider wegen der Pandemie ausgesetzt werden. Die Durchführung war auf Grund der Einschränkungen für Präsenzveranstaltungen nicht möglich. Da diese Formate bislang bei uns noch nicht etabliert waren, ergeben sich daraus zunächst keine zusätzlichen negativen Auswirkungen oder Effekte. Es ist mit einer dauerhaften Erhöhung der Homeoffice-Quote zu rechnen. Die Mitarbeitenden haben sich an die Durchführung von Meetings oder Seminaren bei Video- oder Onlinekonferenz gewöhnt, diese Formate werden sicher in großem Umfang beibehalten. Dies hat Folgen für die interne Kommunikation: Es wird noch schwieriger, Mitarbeitende mit Hilfe von Präsenzformaten zu erreichen, da die Quote der physischen Anwesenheit im Betrieb geringer sein wird.
Frage 4: Welche zeitnahen Veränderungen siehst du grundsätzlich bzgl. der internen Kommunikation?	Ich gehe davon aus, dass auch in Zukunft viele Mitarbeitenden überwiegend im Homeoffice arbeiten werden. Deshalb werden wir uns noch mehr auf Online-Kommunikation konzentrieren. Das umfasst Kommunikation über E-Mail und unsere Intranetkanäle (push und pull) aber auch den vermehrten Einsatz von Online Meetings und Events.	Die Kommunikation über digitale Kanäle – und damit die Informationsflut – wird weiter zunehmen. Um trotzdem mit Themen durchzudringen, die sich an alle Mitarbeitende richten, könnte es sich lohnen, kleinere Zielgruppen zu bilden, um diese gezielter ansprechen und besser erreichen zu können. Möglicherweise wird man hybride Formate weiterentwickeln, um die Teilnahme vor Ort und Remote in einer Veranstaltung zu ermöglichen. Meiner persönlichen Meinung nach funktionieren hybride Formate bislang noch nicht optimal, da Präsenz- und Remote-Teilnehmer die Veranstaltung unterschiedlich wahrnehmen. Es ist de facto keine gemeinsame Veranstaltung und eine Teilnehmerart ist bzgl. der interaktiven Beteiligung benachteiligt.

IWC Schaffhausen	RWE AG	SWITCH
Unsere „Lunch & Learn“-Sessions fallen weg und unser „IT & Security-Tag“ wurde abgesagt. Dies ist aber nicht schlimm, da wir 2018 und 2019 bereits viel gemacht haben. Alle freuen sich nun, dass es wieder losgeht. Wir haben zuerst darauf verzichtet, „Lunch & Learn“ virtuell durchzuführen, da es nicht gepasst hat in einer Zeit, in der beinahe der komplette Arbeitsalltag digital durchgetaktet war. Jetzt im Sommer 2021 haben wir wieder virtuell gestartet und freuen uns über gute Besucherzahlen. Wir hoffen, die Events Ende 2021 wieder physisch durchführen zu können.	Um zu zeigen, wie schnell man selber betroffen sein kann, führe ich viele „Live Hacking“-Sessions durch – bis März 2020 noch vor Ort, nun im Web. Das war eines der erfolgreichsten Awareness-Module unserer Kampagne, da hierbei in einem Rollenspiel vor Publikum echte Angriffsszenarien zwischen Angreifer und Opfer simuliert werden. Da hatte man auch schnell die Aufmerksamkeit des gesamten Publikums, weil man als Teilnehmender mitten im Geschehen ist und stets eine persönliche Betroffenheit erreicht wird. Durch die Einbindung von Umfragetools und Webcams haben wir auch virtuell eine Atmosphäre geschaffen, in der die Kollegen involviert sind und direkt Feedback geben können. Generell habe ich mich in 2020 bzw. 2021 an digitalen Kanälen orientiert. Mit unseren Inhouse-Entwicklern habe ich eine App für Informationsklassifizierungen entwickelt und verpflichtend auf allen smarten Konzerngeräten installieren lassen. Durch die simple Bedienung der App erhalten die Kollegen und Kolleginnen Unterstützung, ob es sich um eine sensible oder nicht-sensible Information handelt und wie mit dieser umzugehen ist.	Alle Maßnahmen, die eine generelle Präsenz vor Ort erfordern, wurden verschoben, digitalisiert oder abgesagt. Der offizielle Start der Kampagne wurde verschoben bzw. abgesagt, da wir schnell reagieren mussten. Dazu haben wir Postkarten mit Logo und Sicherheitstipps für das Arbeiten zu Hause an alle geschickt. Auch die Begleitung der Einführung des neuen Passwortmanagers hatte unter den gegebenen Umständen Priorität. Kommunikation und Unterstützung sind aufwendiger, wenn die Mitarbeitenden nur unregelmässig vor Ort sind. Poster und Workshops sind erst einmal verschoben, das Lunch’n’Learn wird virtuell durchgeführt und der Remote-Working-Guide wie die Postkarte nach Hause geschickt. Zusätzlich waren wir häufiger im monatlichen Unternehmensmeeting präsent. Wir konnten bisher keine Auswirkungen verzeichnen. Es scheint vielmehr so, dass das Thema mehr Aufmerksamkeit bekommt – sowohl von den Mitarbeitenden als auch vom Management. Um die Beziehung zu Arbeitsplatz und KollegInnen nicht ganz einschlafen zu lassen, hat das Management entschieden, alle dazu aufzufordern, an unserem SWITCH Security Awareness Abenteuer „Track The Hacker – die Schnitzeljagd“ teilzunehmen. Unter Einhaltung der Hygieneregeln folgen die Mitarbeitenden in Kleingruppen den digitalen Spuren des Hackers, um die gestohlenen Daten zu retten. Während wir den Mitarbeitenden ein erfrischendes Teamerlebnis ermöglichen, stärken wir das Security-Bewusstsein, knüpfen an unsere internen Regeln an und verbreiten Wissen zum Thema Datenschutz.
Ich denke, 2022 wird alles wieder beim Alten sein. Ende 2021 starten die physischen Events wieder – dann mit einem strengen Schutzkonzept.	Für 2022 lässt mich meine Glaskugel leider im Stich. Was ich jedoch schon in 2020 geändert hatte und beibehalten werde, ist mehr Transparenz in den Ergebnisse von Maßnahmen und dem „Warum?“ Beispiel „Phishing-Tests“: Anhand der Ergebnisse lässt es sich aus Sicht der Cyber Security einfacher argumentieren, warum Phishing eine reale Gefahr ist und nicht etwas diffus „Esoterisches“, das irgendwo anders passiert, „aber doch nicht bei uns!“. Durch die interne Veröffentlichung der Klick-, Eingabe- und Reportingrate ist das Ganze weniger theoretisch und greifbarer für alle.	Alle Maßnahmen, die auf zufällige Beachtung ausgerichtet sind, müssen umgedacht werden. Kommunikation generell muss direkter und gezielter werden. Poster, Flyer zum Mitnehmen, Walk-Bys funktionieren nicht gut, wenn niemand im Büro ist. Stattdessen braucht es vermehrt direkt adressierte Kommunikation, wie Mails, Postsendungen nach Hause oder persönliche Einladungen zu Events. Kommunikation muss den Mitarbeitenden nach Hause folgen.

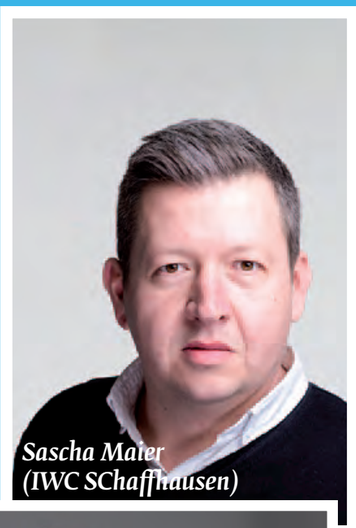
CORONA-UMFRAGE (3/4)

Tool/Anbieter	Amadeus IT Group	Commerzbank AG
Frage 5: Welche Security Awareness-Planungen gibt es konkret für 2021/2022? Ist Awareness für die nächsten Monate überhaupt planbar?	Wir rollen aktuell unser neues Security Awareness Programm auf der „KnowBe4"-Plattform aus. Wir werden hier sämtliche Möglichkeiten nutzen, um unsere Mitarbeitenden kontinuierlich zu schulen und sicherheitsrelevantes Verhalten zu verbessern. Dazu gehören monatliche Kurztrainings, simulierte Phishing-Attacken, Tests und die Bespielung unserer Intranetkanäle mit Security-News, -Tipps und -Videos. Darüber hinaus werden wir weitere Präsenztrainings in Live-Online-Trainings umwandeln und anbieten. Die Roadmap dafür existiert bereits und wir sind jetzt gerade bei der Planung konkreter Termine.	Die Online-Formate werden wie geplant fortgesetzt. Sobald Präsenzmaßnahmen wieder möglich sind, wird die Kampagne um entsprechende, bislang ausgesetzte Formate ergänzt (Security Messe, „Security Arena"). „Ein Spiel aus der Security Arena haben wir testweise in ein digitales Format überführt. Die Beibehaltung des diskursiven Charakters und der Rollout gestalten sich dabei jedoch etwas schwierig.
Kurzbiografie	Thomas Wepner ist seit 1988 in verschiedenen Funktionen für Amadeus tätig. In der Entstehungsphase von Amadeus war er im Netzwerkbereich als Systementwickler für Host-to-Host Protokolle und später als Projekt Manager für die Implementierung von Anbindungen an Airlines verantwortlich. Thomas erweiterte seine Erfahrungen im Management Consulting bei Siemens und als Account Manager bei British Telecom, bevor er seine eigenes Internet Startup gründete. Viele Jahre war er als freier Berater für Projektleitung und Strategieberatung im Netzwerkbereich bei Amadeus tätig. Seit 2014 ist Thomas Teil des CISO Teams von Amadeus. Das Corporate Security Office unter der Leitung von Alain Simon ist verantwortlich für die Definition und Kontrolle der Informationssicherheitsrichtlinien bei Amadeus. Als Senior Corporate Security Officer hat Thomas das globale Information Security Programm aufgebaut und bis Juni 2018 geleitet. Parallel dazu übernahm er 2015 den Aufbau und die Leitung des globalen Security Awareness-Programms. Seit Juli 2018 ist Thomas vollumfänglich für die humanen Aspekte in der Informationssicherheit verantwortlich. Seine Aufgaben umfassen Security Awareness, Training und Kommunikation, sowie alle weiteren Personalsicherheitsmaßnahmen vor, während und nach der Beschäftigung.	Michael Peters, seit 1996 bei der Dresdner Bank bzw. Commerzbank. Bis 2017 in zahlreichen unterschiedlichen Funktionen im Personalbereich der Bank, zuletzt „Information Security Officer" Seite Ende 2017 zuständig für „Information Security Awareness" im zentralen Bereich Group Risk Management / Cyber Risk & Information Security

IWC Schaffhausen	RWE AG	SWITCH
Wir haben beschlossen, alles agil durchzuführen. Im Moment planen wir maxim al 3 Monate im Voraus.	Teils-teils. Es gibt Kanäle der Wissensvermittlung die „Pandemie-resistent" sind. Nehmen wir ein Web-Based-Training, einen Phishing-Test oder eine Intranet-Infoseite, sprich: alles, was digital ist. Auf diese werde ich weiterhin setzten, z. B. in Web-Sessions, etwa Cyber Security-Trainings für Anwender oder fachbereichsspezifische Trainings wie z. B. für HR, Finanzbereiche, etc. Ein klarer Vorteil der Web-Sessions besteht darin, die Beispiele schneller an die Zielgruppe anpassen zu können. Unplanbar sind hingegen alle Trainings vor Ort (etwa echte Live Hackings oder Escape Rooms). Diese Face-to-face-Formate werden erstmal in die Schublade gepackt und – wenn die Randbedingen es wieder zulassen– wieder ein wichtiger Bestandteil unserer Kampagne sein. Die Stärke des „persönlichen Kontakts" sollte nicht unterschätzt werden. Dieser führt dazu, dass die Mitarbeitenden (auch körperlich) spüren, dass man selbst auch ein Mensch ist und nicht ausschließlich als „User" oder „Security-Typ" wahrgenommen wird. Dieses Erspüren ist der Türöffner für alle Cyber Security-Themen. Häufig kommen die Teilnehmenden gerade nach Präsenzformaten auf mich zu und sprechen Themen an, die aus Ihrer Sicht nicht richtig laufen oder fordern von sich aus Security-Inhalte in Bezug auf private Nutzung.	Bisher haben wir das vorliegende Konzept unserer Security Awareness-Kampagne noch nicht konkret anpassen können, da wir hauptsächlich damit beschäftigt waren zu „reagieren" und umzuplanen. Alle künftigen Massnahmen müssen aber, wie unter 4. beschrieben, angepasst werden. Generell müssen wir darauf achten, dass wir flexibel bleiben und auch spontan umdisponieren können. Ein Event ist super, aber immer mit virtueller Backup-Lösung; zusätzlich zu einem generellen Aufruf braucht es eine Mail an jeden Mitarbeitenden; wird Print-Material erstellt, muss Budget für den Versand eingeplant werden. Also: Ja, Awareness für die nächsten 12 Monate ist planbar – wenn für alle Massnahmen ein virtueller Plan B mitgedacht wird.
Sascha Maier ist CISO von IWC Schaffhausen, dem bekannten Luxusuhren-Hersteller aus Schaffhausen. In seiner Funktion ist Sascha Maier verantwortlich für die komplette IT- & Informationssicherheit der IWC an allen Standorten. Durch das Setzen von Sicherheitsstandards, die Bewertung von Sicherheitsrisiken und die Umsetzung von Gegenmassnahmen sichern er und sein Team die Infrastruktur. Zudem wird bei der IWC seit Jahren aktiv das Thema User Awareness und Cyber Intelligence vorangetrieben.	Fabian Cholewa ist Awareness & Cyber Security Manager bei der RWE AG, bei der er eine multikulturelle Awareness Kampagne etabliert und stetig weiterentwickelt hat, um alle Mitarbeitenden des globalen Energieversorgers hinsichtlich Cyber Security-Themen zu sensibilisieren. Um dies zu erreichen, nutzt er verschiedene Kanäle des Wissenstransfers. Neben klassischen WBTs oder einer Intranet-Präsenz greift er zu interaktiven Formaten, z.B. „Live-Hackings" oder „Escape Rooms", um so in den Dialog mit den Menschen zu gelangen. Derartige Standorte für Präsenzformate werden u. a. infolge von Ergebnissen aus regelmäßigen Phishing-Tests sondiert. Cholewa ist besonders wichtig, dass Cyber Security im beruflichen und privaten Alltag intrinsisch wirkt. Darum legt er viel Wert auf Transparenz und dem „Reason Why".	Als Security Awareness-Spezialistin bei SWITCH setzt sich Katja Dörlemann für den Faktor Mensch in der Informationssicherheit ein. In Zusammenarbeit mit der Schweizer Hochschullandschaft und Internet-Community unterstützt sie Internetnutzende dabei, sich online sicherheitsbewusst zu bewegen und mündige Entscheidungen im Umgang mit den eigenen Daten zu treffen. Katja sammelt seit fast 10 Jahren Erfahrungen in Awareness und doktorierte in Allgemeiner und Vergleichender Literaturwissenschaft an der Universität Zürich. Cornelia Puhze ist Communications Managerin bei SWITCH. Gerüstet mit einem MA in Political Communications, Goldsmiths, lernte sie ihr Handwerk in Privatwirtschaft, im öffentlichem Sektor und in NGOs in Zürich und London. Von der Umsetzung der Awareness@SWITCH Massnahmen inspiriert, bildete sie sich weiter zur SANS Security Awareness Professional (SSAP).

TEILNEHMER/INNEN
DER CORONA-UMFRAGE

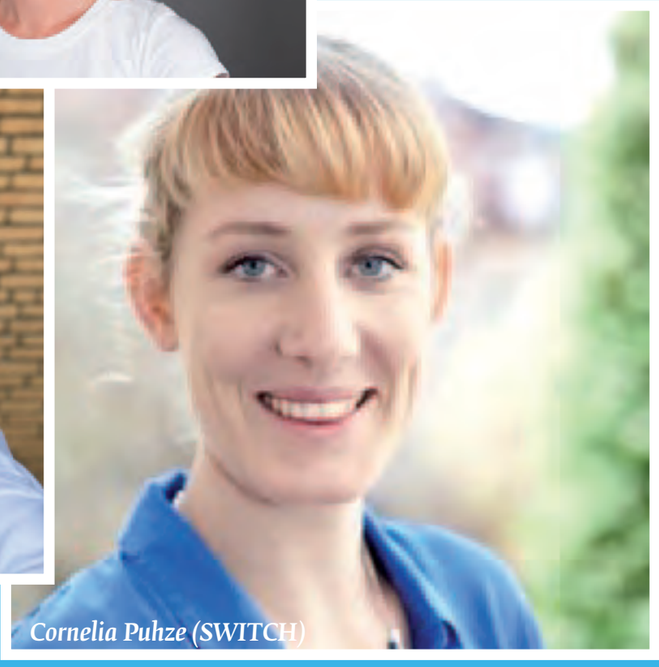
Michael Peters (Commerzbank)


Sascha Maier (IWC SChaffhausen)

Kris Harms

Katja Dörlemann (SWITCH)

Fabian Cholewa (RWE)


Cornelia Puhze (SWITCH)

CORONA-UMFRAGE (4/4)

„DANN BLEIBT DIE BLUSE EBEN UNGEBÜGELT IM SCHRANK.“

NOCH EIN INTERVIEW – MIT KRIS HARMS

Kris, wie geht es dir? Was hat sich m Laufe der Pandemie in deinem Job geändert? Haben sich infolge von Corona z. B. Beziehungen innerhalb deines Teams oder mit Vorgesetzten auffällig verändert?
Absolut positiv, da ich nun komplett aus meinem Homeoffice arbeiten kann. Das gibt mir mehr Flexibilität. Gleichzeitig muss ich darauf achten, genug Pausen zu machen, wenn es hoch her geht. Das Setup entspricht vollends meinem Naturell, da ich es gewohnt bin, selbstständig zu arbeiten und mich sehr gut selbst motivieren kann. Ich kann meine Lieblingsklamotten anziehen und muss z. B. keine Blusen bügeln. Wenn die Situation so bliebe, könnte ich die Hälfte meiner Garderobe entsorgen. Der spontane Austausch mit Kunden bzw. Kollegen und Kolleginnen fehlt nach über einem Jahr ein bisschen. Aber wenn ich das Bedürfnis habe mich auszutauschen, rufe ich einfach an und verbinde das mit einem Spaziergang in der Natur

Vor welchen besonderen Herausforderungen steht die Security Awareness derzeit bei deinen Kunden? Wie unterscheiden diese sich zu denen vor März 2020?
Nach wie vor im Fokus stehen bei meinen Kunden globale Abdeckung, Wirksamkeit also auch Messbarkeit und Dokumentation aller Maßnahmen. Zudem die Bündelung von Know-How aus unterschiedlichen Standorten, um dieses allen Mitarbeitern zugänglich zu machen. Noch stärker als bisher steht die Digitalisierung von Schulungen im Vordergrund bzw. der Austausch über Online-Plattformen.

Welche Security Awareness-Maßnahmen wurden in den letzten Monaten in deinem Unternehmen durchgeführt und wie unterscheiden die sich zu denen im Vorjahr bzw. denen im Januar/Februar 2020?
Die Krise hat einmal mehr gezeigt, wie wichtig sensibilisierte Mitarbeiter sind! Gerade im Homeoffice gibt es andere Anforderungen an Daten- und Informationssicherheit. Meine Kunden haben diesbezüglich sehr viel Aufklärungsarbeit geleistet und verständliche Handlungsempfehlungen an ihre Mitarbeiter ausgegeben. Bei einem meiner Kunden war der letztjährige Security Awareness Month im Oktober so erfolgreich, wie noch nie. Das lag vor allem daran, dass lokale Präsenzveranstaltungen durch Online-Events ersetzt wurden, die allen Mitarbeitern weltweit offenstanden.

Welche zeitnahen Veränderungen siehst du grundsätzlich bzgl. der internen Kommunikation?
Die Kommunikatoren im Unternehmen stehen vor der Herausforderung, den Mitarbeitern weiterhin ein „zu Hause“ zu geben. Der Digital Workplace wird weiter in den Fokus rücken, also der Ort, an dem relevante Informationen verfügbar und Austausch mit Kollegen möglich ist. Darüber hinaus, sehe ich jede Führungskraft im Unternehmen in der Verantwortung, „seine“ Mitarbeiter an Entwicklungen im Unternehmen teilhaben zu lassen. Offener Austausch ist wichtiger denn je, auch über den eigenen Tellerrand hinaus. Der Unterschied zwischen echten Führungskräften und bloßen „People“-Managern wird sich jetzt zeigen. Kommunikation findet auf allen Ebenen statt und ist eben nicht nur der Job der Kommunikationsprofis im Unternehmen. Leider wird diese Verantwortung allzu oft auf diese abgewälzt. Nach dem Motto „Dafür ist doch die Kommunikationsabteilung zuständig“.

Welche Security Awareness-Planungen gibt es konkret für 2021/2022? Ist Awareness für die nächsten Monate überhaupt planbar?
Awareness-Maßnahmen sind m.E. für jedes Unternehmen, das Personal- und/oder Kundendaten verarbeitet, unabdingbar und sollten deshalb immer in die Jahresplanung aufgenommen werden. Die Kreativität der Verantwortlichen ist gefragt, wenn es darum geht, geplante Präsenzschulungen oder -veranstaltungen ins Netz zu verlegen. Da gibt es m.E. gute Möglichkeiten, Formate und Ideen, um das Thema interaktiv und spielerisch zu vermitteln.

Kris Harms ist seit vielen Jahren als Freelancer in den Feldern Kommunikation, Training, Projektmanagement tätig, u. a. für die Allianz SE.

AWARENESS-OSPA STATT „SENSIBLISIERUNGS-OPA“

DR. CHRISTOPH SCHOG, EX-T-SYSTEMS INTERNATIONAL, MIT DEM OSPA FÜRS LEBENSWERK GEWÜRDIGT

VON DIETMAR POKOYSKI

Dr. Christoph Schog, geboren 1955 in Köln, heute lebend in Aachen, hat von 1974 bis 1981 an der RUB bzw. RWTH Aachen Ingenieurwesen studiert. Von 1988 bis 2003 war er Consultant bei der GEI, die 1990 vom debis Systemhaus, einer Daimler-Tochter und seinerzeit der größte deutsche IT-Dienstleister, eingekauft wurde. Dort war er als Berater bzw. Coach bei der Modellierung der Architektur von IT-Systemen tätig, etwa als Trainer für Methoden und Tools im Bereich von Software-Engineering (SA/RT/MD) bzw. als Line Security Officer für Software Entwicklungsbereiche von T-Systems, die 2002 die debis übernahm. Von 2004 bis 2009 war Schog CSO bei T-Systems, seit 2009 Executive Security Manager. In dieser Position entwickelte er – den Anforderung eines Rollenwechsels bei Security Managern in den Nullerjahren entsprechend – zunehmendes Interesse für Security-Kommunikationsthemen mit den Rollen „International Security Management, Executive Security-Representative of T-Systems, Security-Awareness-Expert“.

Hinter den offiziellen Schreibweisen von Schogs vielfältigen Security-Rollen wird bei genauer Betrachtung schon früh die Entwicklung zum Security-Kommunikator bzw. Awareness-Streetworker gewahr, der interne Audits bei den weltweiten T-Systems--Units und seine internationale Partnerschaften sowie seine ausgesprochen gute internen wie externen Vernetzungen stets dazu nutze, die Menschen aus seiner Umgebung für Sicherheitsthemen auch en passant zu sensibilisieren, ohne dass sein großes Sendungsbewusstsein bemerkt wurde.

Überhaupt war Schog neben Munich Re (MR) oder RWE, einer der ersten, der komplette Awareness-Kampagnen in deutschen Konzernen etablierte. 2004 startete er mit „Mission Security“ das erste Sensibilisierungsprogramm innerhalb der Telekom Group, basierend auf der vermutlich ersten Awareness-Leitfigur eines deutschen Unternehmens, James Bit, einer Schattenfigur, die einem nach der Betrachtung nicht mehr aus dem Kopf ging.

2010 bzw. 2014 folgten weitere Kampagnen zu einem Zeitpunkt, als T-Systems – getrieben von Schog – Awareness bereits als dauerhaftes Engagement betrachtete, 2010 verknüpft mit dem Moderationskartenset, „mySecurity & Privacy Box“ und dem Lernstationsformat „SECURITY PARCOURS“, 2014 mit „Card of the Month“, bei der 4 Jahre lang jeden Monat zu 48 Themen diverse mehrsprachige Formate erschienen waren. Darüber hinaus konnte Schog in den 13 Kampagnenjahren bis 2017 mehr als 200 verschiedene Awarenessformatel aunchen. In diesen 13 Jahren hielt er weltweit mehr als 100 Fachvorträge und besuchte hunderte T-Systems-Standorte, um bei Inkubation vorort zu unterstützen.

Zu seinem Engagement gehörte 2006 die Gründung der wichtigsten Awarenessinitiative deutscher Unternehmen, dem „Dax-30-Roundtable Security Awareness“ mit Michael Lardschneider (MR) oder Klaus Altmeyer (BASF). Schog gehört dieser Initiative, bei der regelmäßig während Präsenzmeetings Good-Practice-Sharing betrieben wird, seit Mitbegründung an, war stets einer ihrer Treiber und hat immer wieder für eine Auffrischung durch aktives Anwerben „jüngerer“ Teilnehmer betrieben.

2017 übergab Schog, der sich privat im Westdeutschen Kanuverband und dort vor allem in der Jugendarbeit engagiert, das Thema Awareness bei T-Systems an einen Konzernkollegen. Im Mai 2021 wurde er bei T-Systems in den Ruhestand verabschiedet.

Schaut man auf die Entwicklung als CSO, fällt auf, dass Schog sich von einem technisch orientierten Security-Experten zum Fachmann in Human-Based-Security entwickelt hat. In Bezug auf produktive Ansprache halfen technischen Kenntnisse und seine Fähigkeit, den technischen Kontext sprachlich auszudrücken, hinsichtlich seiner Mission, die Menschen von der zunehmenden Bedeutung der Security-Kommunikation zu überzeugen, eine Art (guter) „Wolf“ im „Schafspelz, der infolge seiner Gewandtheit in beiden Securitywelten besonders viele Multiplikatoren und Mitstreiter gewinnen konnte.

So ist es ihm auch gelungen, komplexe Programme, die nicht nur Wissensvermittlung dienten, mithin solche mit hohen Marketinganteilen, emotionaler Ansprache und beeindruckenden, involvierenden Narrativen, zu einem Zeitpunkt einzuführen, als andere den Awarenessbegriff noch nicht einmal buchstabieren konnten. Als Erfolgs-Beleg förderte er die Entwicklung eines Security-Awarenss-Index und führte diese empirische Evaluationsmethode 2005 bei T-Systems ein.

Seine Kampagne „Mission Security“ mit der bloggende Agentenleitfigur James Bit wurde 2007 mit dem Sicherheitspreis Baden-Württemberg ausgezeichnet. Ab 2009 nutzte Schog auch Elemente systemischer Kommunikation, indem er Führungskräfte Sicherheitsthemen als diskursive Elemente in Teamsettings integrieren ließ. Beim Sprechen über Sicherheit sollten 70 Moderationskarten helfen, Diskussionen vorzubereiten – eine innovative Sicherheitskultur-Modellierung.

2011 kam als diskursiv-systemische Elemente die Lernstationen des „SECURITY PARCOURS“, Minigames „out of the Box“, hinzu, bei der Telekomkollegen mit Teams Security-Simulationen spielend erörtern. 2013 wurde dieses Format vom ISF als „Most innovative Awareness-Campaign“ ausgezeichnet.

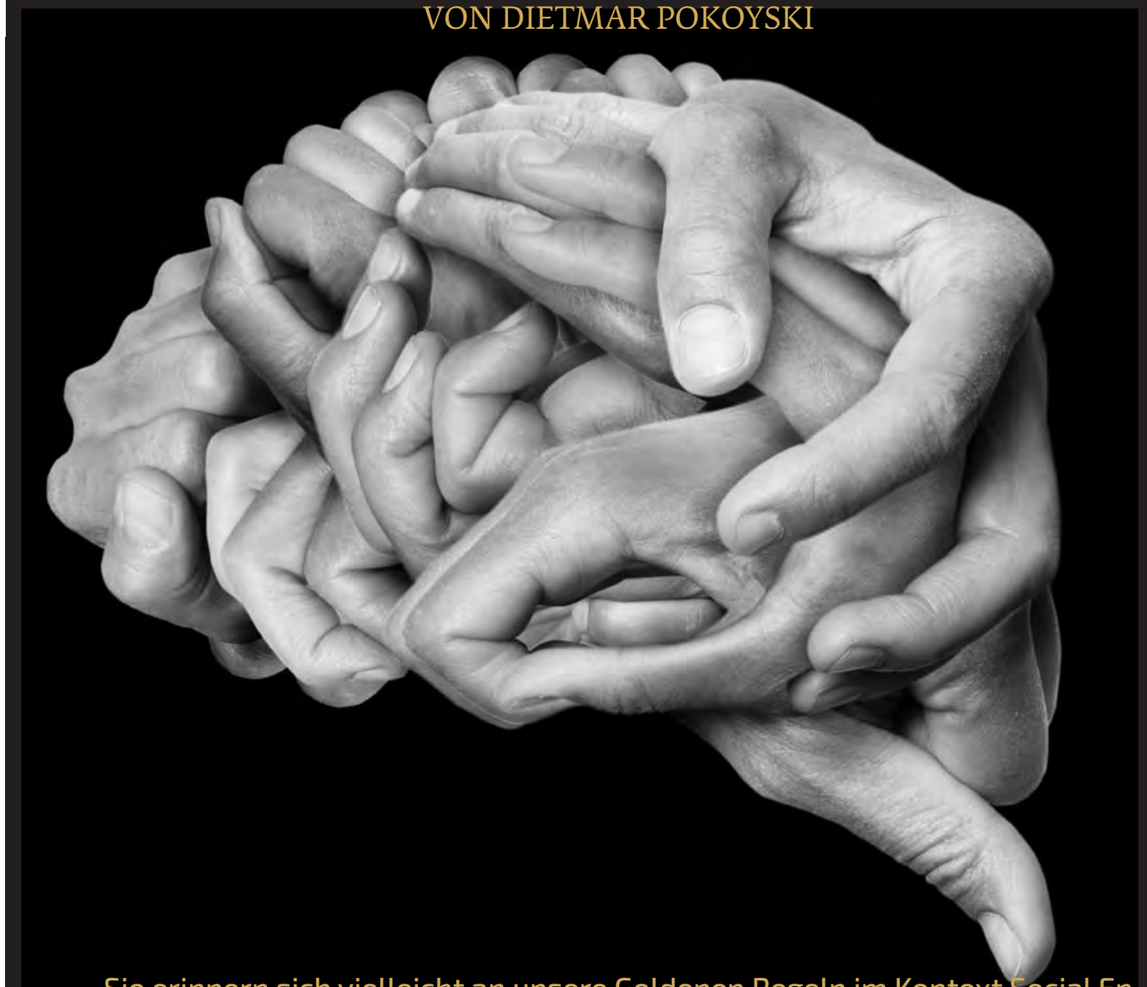
Die Liste gamifizierte Formate, derer sich Schog als erster Awarenessmanager hierzulande bediente ist aber noch länger. Hierzu gehören das begehbare Social-Engineering-Teppichspiel „Bluff&Hack“ oder das Risikomanagement-Workshopformat für Management-Boards, „Security Spot“. 2015 entwickelte Schog einen Awareness-KPI mit einer innovativen Balanced-Score-Card. 2016 erstellte er das weltweit erste integrative Security-Awareness-Framework, in dem Aspekte von Informationssicherheit, Didaktik, Marketing, Kommunikation und Psychologie als Standard für T-Systems geregelt sind.

Diese Instrumente teilte er großzügig mit anderen Awarenessverantwortlichen, insbesondere mit dem „Dax-30-Roundtable Security Awareness“. Gerade seine menschliche Wärme mit seiner Offenheit gegenüber Innovationen, Kooperationen, dem Teilen und seiner Großzügigkeit, nicht nachzurechnen, dass er deutlich mehr seiner Ideen geteilt hat als ihm umgekehrt zurückgegeben wurden, machen ihn sympathisch und populär. Man kann sicher behaupten, dass es heute kein Unternehmen in Deutschland gibt, das nicht auch Methoden bzw. Tools einsetzt, die Schog nicht zumindest mitentwickelt hätte. Es steckt also überall, wo Sensibilisierung passiert, ein Schog mit drin. Insofern gibt es niemanden, auf den ein Kosename wie „Mr. Awareness“ besser passen würde als auf ihn.

INKOHÄRENZ & VERLETZLICHKEITSPARADOX

NUR WER NICHT 100%IG ABDICHTET, KANN AUF AWARENESS ZÄHLEN

VON DIETMAR POKOYSKI



Sie erinnern sich vielleicht an unsere Goldenen Regeln im Kontext Social Engineering? Wenn wir – bei unserem Gegenüber kognitiv oder rein intuitiv, d. h. über unser Bauchgefühl – die drei Kommunikationslayer, die verbal-informellen, die nonverbalen oder aber die paraverbalen, als inkongruent wahrnehmen, stimmt etwas nicht mit unserem Gesprächspartnern. Zum Beispiel wenn sich jemand selbstsicher gibt und dabei nervös mit dem Fuß zappelt. Dies kann – muss aber nicht – ein Hinweis darauf sein, dass die Motive des Gegenübers andere sind, als die, die er oder sie vordergründig darzustellen versucht. Wir empfehlen dann, vor allem wenn es sich beim Gegenüber um eine/n Fremde/n handelt, besonders aufmerksam zuzuhören – und zwar mit allen „Ohren", auch mit dem, durch das unser Bauch „hört".

Wege aus der Angst führen zu Entwicklungssprüngen

Aus „Wege aus der Angst" (Vandenhoeck & Ruprecht), dem neuen Buch des Hirnforschers Gerald Hüther, vielleicht der einzige Neurobiologe, dem ich traue, weil er als einer der wenigen in der Lage ist, durchdringend über den Tellerrand seiner Kerndisziplin zu blicken, habe ich gelernt, dass wir Menschen selber Inkohärenz brauchen, um uns zu entwickeln.

Wir lernen nur dann etwas hinzu, wenn unser Zustand von Kohärenz, die unser Gehirn zwar anstrebt, weil es dann weniger Energie verbraucht, erschüttert wird. Erst wenn die „Harmonie" unserer Existenz aus dem Gleichgewicht gerät, z. B. durch Angst, die auch Angriffe oder Fehlleistungen impliziert, findet eine (Rück-)Verwandlung in einen weniger energieaufwändigen Zustand statt. Nur durch diesen „Kniff" sind wir in der Lage, aus Fehlern zu lernen, diese aufgrund unserer Kompetenz, die wir mit zunehmender Risiken und damit verbundener Fehlerhäufigkeit herausbilden, korrigieren zu können.

Für die Sicherheitskultur bedeutet dies, dass die Mitarbeiter einer „gut" geschützten Organisation didaktisch auf Sparflamme agieren und gegebenenfalls bei Zuspitzung von Risiken aus sich heraus weniger reaktionsschnell mit Korrekturen reagieren können als solche, die häufiger oder ständig im Fokus von Cyberangriffen stehen oder infolge risikoreicher Tätigkeiten regelmäßiger mit eigenen Fehlleistungen konfrontiert sind.

Verletzlichkeitsparadox als Trigger für Security Awareness

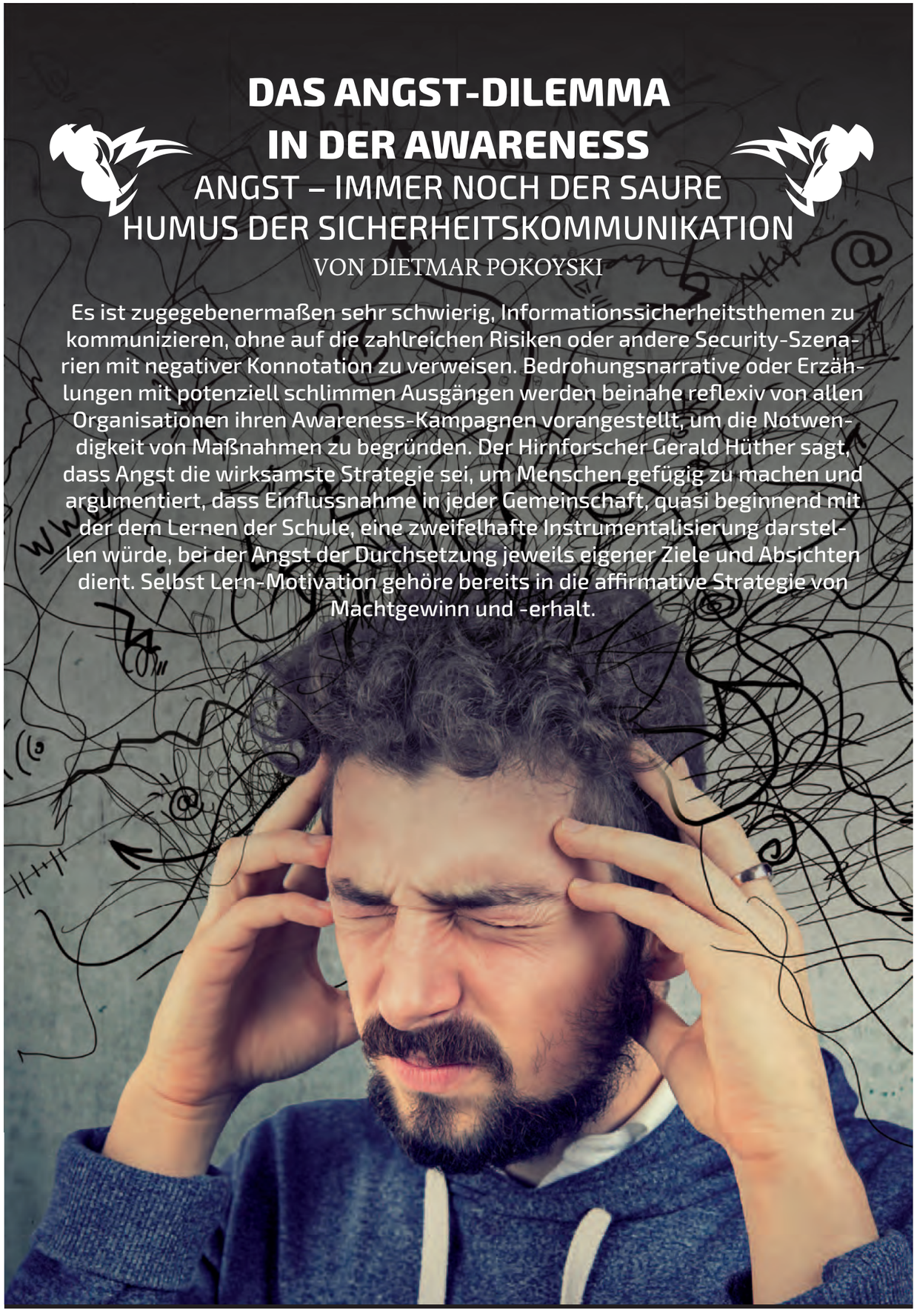
Wenn man in diesem Kontext noch das Verletzlichkeitsparadox betrachtet – d. h. je „besser" eine Organisation geschützt ist, desto verwundbarer ist sie im Falle eines Incident, umso mehr drängen die Geschützen, die sich durch Sicherheitsmaßnahmen ggf. stillgelegt fühlen, darauf „auszubrechen" – ergibt sich aus der Addition beider hier betrachteter Phänomene das vielleicht beste Argument für Security Awareness in Abgrenzung zur Überhöhung einer Abdichtungsphilosophie aus der klassischen, technisch oder prozessual orientierten IT-Security. Denn durch das Verletzlichkeitsparadox verschärfen sich die Vorfall- und Schadens-Risiken, weil es sich sozialpsychologisch unmittelbar auf Informationssicherheit auswirkt. Das heißt: Die Risiken erhöhen sich auch dadurch, dass das Verhalten von Menschen, die an Schutz und Sicherheit gewöhnt sind, durch den wachsenden Anspruch, die Sicherheit delegieren und eben Schutz durch Dritte erwarten zu können. Gleichsam sinkt die Motivation, selbst aktiv zu werden und z. B. am Schutz von Informationen selbst aktiv mitzuwirken. Wie man es auch dreht: Inkohärenz und Verletzlichkeitsparadox sind die extradisziplinären Belege dafür, dass 100%ige Sicherheit nicht möglich ist und auch nicht angestrebt werden sollte. Der Mensch ist die Lücke im System, jedoch eine notwendige, eine lebende und daher selbstlernende Lücke, um aus ihr heraus am Ende mehr Sicherheit statt weniger erzielen zu können. *Erstveröffentlichung im „Blogdown Awarehousemeister" auf known-sense.de*

DAS ANGST-DILEMMA IN DER AWARENESS

ANGST – IMMER NOCH DER SAURE HUMUS DER SICHERHEITSKOMMUNIKATION

VON DIETMAR POKOYSKI

Es ist zugegebenermaßen sehr schwierig, Informationssicherheitsthemen zu kommunizieren, ohne auf die zahlreichen Risiken oder andere Security-Szenarien mit negativer Konnotation zu verweisen. Bedrohungsnarrative oder Erzählungen mit potenziell schlimmen Ausgängen werden beinahe reflexiv von allen Organisationen ihren Awareness-Kampagnen vorangestellt, um die Notwendigkeit von Maßnahmen zu begründen. Der Hirnforscher Gerald Hüther sagt, dass Angst die wirksamste Strategie sei, um Menschen gefügig zu machen und argumentiert, dass Einflussnahme in jeder Gemeinschaft, quasi beginnend mit der dem Lernen der Schule, eine zweifelhafte Instrumentalisierung darstellen würde, bei der Angst der Durchsetzung jeweils eigener Ziele und Absichten dient. Selbst Lern-Motivation gehöre bereits in die affirmative Strategie von Machtgewinn und -erhalt.



Durch das Bedürfnis, Teil einer Gemeinschaft zu sein, nehmen wir die meisten von uns die Unterdrückung hin und erreichen dennoch nie das Ziel, werden durch die Instrumentalisierung, Manipulation und Ängste selbst zu einsamen Einzelkämpfern, die in Ihrer Verzweiflung des Scheiterns ihre selbstbezogenen Vorstellungen verwirklichen wollen, indem sie Macht über andere erlangen. So schaffen wir eine Gesellschaft von Angstmachern und Unterdrückten. Dies ginge sogar soweit, dass die Angstmacher die natürlich vorhandene Resilienz ihrer Opfer bewusst schwächen. In der Security wird dies sichtbar in Organisationen, in denen man den Mitarbeitern die Kompetenz abspricht, sich selbst zu schützen und sich so technisch bzw. prozessual aufrüstet, dass aus Notwehr der Opfer Delegation wird und man sich selbst nicht mehr kompetent und daher auch verantwortlich dafür fühlt, die eigene Organisation zu schützen. Hüther sagt auch: „Je lebensuntüchtiger ein Mensch durch die ständige Nutzung Sicherheit suggerierender Gerätschaften und Hilfsmittel geworden ist, desto leichter lässt er sich durch die Ankündigung einer bevorstehenden Bedrohung in Angst und Schrecken versetzen (Wege aus der Angst, S. 78-79).

Schuld, Scham und Angst – das Security-Dreigestirn des Horrors

Gerade in der Security Awareness setzen wir gerne Geschichten um Fehlleistungen bzw. mögliche Folgen von Vorfällen ein, z. B. dass die Existenz eines Unternehmens bedroht ist, wenn man vertrauliche Informationen preisgibt oder dass man Opfer von Erpressern wird und seine komplette Datenidentität aufs Spiel setzt, sobald man E-Mails von unbekannten Absendern öffnet, die ggf. Ransomware oder andere Schadsoftware enthalten. Auch Awareness-Videos, Erklärfilmchen oder andere Sensibilisierungs-Narrative arbeiten häufig in diese Richtung. So gesehen, ist auch der Einsatz von z. B. einer Phishing-Simulation ein typischer Angstmacher. Und Probanden unserer tiefenpsychologischer Studien haben uns erzählt, dass selbst die Meldung eines Vorfalls, z. B. im Kontext Social Engineering, eine Meldung, die eigentlich produktiv auf die Resilienz von Organisationen einzahlen sollte, nicht nur Schuld und Scham bei ihnen auslöst, sondern eben auch angstbesetzt sei. Die meisten Unternehmen behaupten lediglich, dass sie in Bezug auf Awareness nicht mit dem Zeigefinger agieren. In Wirklichkeit ist ihnen gar nicht bewusst, wie sehr sie das Angstsystem der Unterdrückung bereits verinnerlicht haben.

Vom Teppichhändler zum Streetworker

Aber was können wir als Awareness-Streetworker, die nicht nur Fertigprodukte in den Markt drücken wollen, um Sensibilsierung wie Teppiche zu verticken, tun, um uns von den Angstmachern abzugrenzen und die leidvolle Kette der Angst zu unterbrechen? Schaffen wir es überhaupt, auf Darstellung von Risiken zu verzichten, um unsere Maßnahmen nachvollziehbar zu erklären und zu begründen? Ich würde sagen, nein, das geht vermutlich nicht. Schon die Weltreligionen sind daran gescheitert, die Angst der Menschen, die ihnen folgen, zu beschwichtigen. Im Gegenteil! Aber wir können uns von Maßnahme zu Maßnahme, von Kampagne zu Kampagne bewusster machen, was die Aufrechterhaltung von Angstbildern mit Menschen anstellt – und genauso, wie es ein Prozess ist, sich Klimaschutz und Tierwohl und damit verbundene, notwendige Veränderungen Stück für Stück bewusster zu machen, sollten wir ab und an raustreten aus dem Angstmacher-Hamsterad und uns auf eine Metaebene begeben, von der aus wir in den Diskurs mit der Zielgruppe, den Mitarbeitern, gehen, um genau das Dilemma, das ich hier beschreibe, zu diskutieren.

Wer Angst schürt, zerstört langfristig genau das, was er dadurch aufrechtzuerhalten versucht

Awareness braucht das Prinzip „Talking Security“ – entlang dieses Dilemmas umso mehr. Außerdem ist selbstbestimmtes Arbeiten eh ein großes Thema – beschleunigt durch die Home Office-Kultur infolge der COVID-19-Pandemie. Statt sog. ‚innovative‘ Apps der internen Kommunikation einzuführen, um die Menschen bei der „Heimarbeit“ wieder einmal zu kontrollieren, sollten wir mit ihnen diskutieren, wie Arbeit 2030 aussehen könnte und wie wir trotz zunehmender Digitalisierung und damit verknüpfter Risiken Informationssicherheit gewährleisten können, am besten gemeinsam und ohne Angst. Dafür braucht es starke Sicherheitsbilder jenseits von Kapuzenträgern und anderer düsterer Angstmacherei, produktive Bilder, die auf die Benefits von sicherem Verhalten einzahlen und eben den Austausch auf Augenhöhe gewährleisten – wieder mal frei nach dem bekannten Awareness-Motto „Wir haben keine Chance – also nutzen wir sie.“ Oder um es mit Gerald Hüther zu sagen: „Wer Angst schürt, zerstört langfristig genau das, was er dadurch aufrechtzuerhalten versucht.“ *Erstveröffentlichung im „Blogdown Awarehousemeister“ auf known-sense.de*

DIE AUTOREN/INNEN & HERAUSGEBER

MICHAEL

MARCUS

KATJA

VLAD

STEFFEN

DIETMAR

UWE

MARKUS

Marcus Beyer *wechselte 2020 nach mehr als 15 Jahren als Berater im Thema Security Awareness in eine interne Rolle zur Swisscom (Schweiz) AG als Security Awareness Officer und verantwortet dort alle Aufgaben rund um die Sensibilisierung für Securitythemen aus der physischen und logischen Welt. Zudem entwickelt und gestaltet er auch die Trainings für alle Mitarbeitende wie auch die spezifische Ausbildung von Mitarbeitenden mit einer Rolle in der Security. Dabei liegt bei ihm der Fokus immer auf der Entwicklung einer konsequent gelebten Sicherheitskultur, dem Change Management, einer nachhaltigen Kommunikation, „human centered security" und der Interaktion mit Menschen. 2010 haben sich die beruflichen Wege von Katja und Marcus in der Schweiz gekreuzt.*

Dr. Katja Dörlemann *setzt sich als Security Awareness Spezialistin bei SWITCH (www.switch.ch) für den Faktor Mensch in der Informationssicherheit ein. In Zusammenarbeit mit der Schweizer Hochschullandschaft und Internet-Community unterstützt sie Internetnutzende dabei, sich online sicherheitsbewusst zu bewegen und mündige Entscheidungen im Umgang mit den eigenen Daten zu treffen. Katja sammelt seit fast 10 Jahren Erfahrungen auf dem Gebiet der Security Awareness und doktorierte in Allgemeiner und Vergleichender Literaturwissenschaft an der Universität Zürich.*

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.*

Dr. des. Steffen Hessler *(steffen.hessler@rub.de) ist Absolvent des IT-Security-Forschungskollegs „SecHuman – Sicherheit für Menschen im Cyberspace" und Wissenschaftler an der Ruhr-Universität Bochum. Während des SecHuman-Projekts hat er u. a. beim Bundeskriminalamt gearbeitet und Textanalysen und -vergleiche durchgeführt. Im Rahmen dieser Forschungsarbeit schrieb er seine Dissertation zur Autorschaftserkennung im Zusammenhang mit IT-Security Awareness und Prävention von Desinformation und Social Engineering. Steffen Hessler beschäftigt sich seit über 15 Jahren mit Textanalysen und bietet forensisch-linguistische Analysen für Unternehmen an. Weiterhin befasst er sich mit der Vermittlung von IT-Security Awareness-Inhalten mithilfe von Konzepten der Einfachen Sprache.*

Vladyslav (Vlad) Moyerer*, nach seinem Bachelorstudium der Betriebswirtschaftslehre an der Hochschule Niederrhein mit dem Schwerpunkt International Management absolvierte er den berufsbegleitenden Masterstudiengang „Digital Business Managements" an der RFH Köln. Heute ist er als Business Development Manager bei mybreev tätig. Zudem verantwortet er den Social-Media Auftritt des Fachkanals „Corporate Security TV" und ist Membership Officer bei ASIS Germany e.V.*

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 und 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.*

Markus Wagemann*, Markus Wagemann ist seit 2020 bei der mybreev GmbH als Channel Manager beschäftigt. Er ist für den Standort Future Safe House in Essen und darüber hinaus für Netzwerkarbeit sowie Beratung zuständig. Die Themen Nachhaltigkeit, Diversity und new work gehören zu seinen Fachgebieten.*

AWARENESS DARTS:
TREFFEN SIE IHRE TREIBER & -ZIELE

Quelle: known_sense 2019

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: Shutterstock außer S. 5 (Security Awareness Insider) | S. 6, 9 (Fabula Games) | S. 15-17 (einzelne Care4Aware-Gewinner) | S.13 (mybreev) | S. 21-23, 41 (known_sense) | S. 25, 34 (The OSPAs bzw. Christoph Schog) | S. 32, 40 (einzelne Autoren)

TAKE AWARE 2022 # 04

Die Security Awareness-Konferenz

MOTTO: »SIEHE, ACHTSAM SOLL'S VOM HIMMEL REGNEN.«

Care4Aware
Der Security Awareness-Award

FEAT. BRANDING WORKSHOP DAY
»SEXY SECURITY«

28.–29. APRIL 2022 | ESSEN | DEXTRADATA

WWW.TAKE-AWARE-EVENTS.COM

Konferenz-Veranstalter

mybreev

known_sense
awareness you can touch.

TAKE AWARE
Die Security Awareness-Konferenz
www.take-aware.com

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

Medienpartner

CORPORATE SECURITY TV

<kes>
Die Zeitschrift für Informations-Sicherheit

SecuMedia
Der Verlag für Sicherheits-Informationen

Security Awareness Insider

Partner

DextraData

HECOM