TAKE AWARE

SEC&LIFEMAGAZINE

EDITION TAKE AWARE 05

2022 | 4. JG

SONDERTEIL: DOKU MIT DEN FINALISTEN

CARE 4 AWARE

MOTTO: »SIEHE, ACHTSAM SOLL'S VOM HIMMEL REGNEN – AWARENESS & GIESSKANNENPRINZIP«

VOLLE KANNE – (POST)PANDEMISCHE TENDENZEN INTERNER KOMMUNIKATION | FEUCHTE SIEGERTRÄUME – CARE 4 AWARE-FINALISTEN 2022 | BEGOSSENE PUDEL – PASSIVE AGGRESSION ALS SICHERHEITSRISIKO | HIMMLISCHE BOX – DIE SECURITY AWARENESS LIBRARY | ALARM – SENSIBILISIERUNGS-REGEN FÜR KMU | BSI-MYZEL – DAS CYBER-SICHERHEITSNEZWERK UND ANDERE PRÄVENTIONS-GEFLECHTE

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

SEXY SECURITY
SECURITY BRANDING & CREATIVE CAMP
www.take-aware.com

Herausgegeben von

mybreev

known_sense
awareness you can touch.

Medienpartner

CORPORATE SECURITY TV

CONTENT

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

Abbildungen: S. 1 (Titel) Shutterstock | S. 2, 4, 7, 13 Freepik | S. 9-11 Deutsche Telekom AG & mybreev| S. 18 ALARM Informationssicherheit (TH Wildau und Projektpartner (davon S. 18, 20 known_sense) | S. 22-25 BSI | S. 26, 27, 29, 30 known_sense | S. 12-17 einzelne CARE 4 AWARE-Bewerber | S. 28 einzelne Autoren

VOLLE KANNE DIGITAL?

Liebe TAKE AWARE-Community, verehrte Awareness-Freunde & -Freundinnen,

die 5. Ausgabe unseres Magazins präsentiert mit den Finalisten der 2. Auflage des Care 4 Aware-Award erstmals Maßnahmen, die beinahe ausschließlich während der Pandemie entstanden sind oder ausgerollt wurden. Vergleichbar mit Kommentaren bei Fußballspielen, bei denen ein Team nicht in Bestbesetzung auftritt, können wir auch in diesem Kontext konstatieren: „Mit einem solchen oder ähnlichem Portfolio wird in Zukunft vermutlich keine Awareness-Kampagne mehr auflaufen.“ Denn selbstverständlich hat sich über die Pandemie und in den hoffentlich ersten Monaten postpandemischer Vorspielchen die interne Kommunikation erheblich verändert. Nur wie genau? D. h. welche offenen bzw. weniger-sichtbaren, impliziten Veränderungen waren oder sind in der Kommunikation für Mitarbeitende wahrzunehmen? Welche kommen?

Tools der internen Kommunikation wurden in einem nie vergleichbaren Ausmaßes digital ausgerollt – contentgetriebene Portale, WBTs, Apps & Co sind die Pandemie-Gewinner – scheinbar!

Vielleicht ist „digital“ ja die neue Kanalisation? Denn unser professionelles Kanalnetz war ursprünglich eine Präventivmaßnahme im Kontext einer anderen, überwundenen Pandemie, der Cholera. Eher nicht, denn digitale Instrumente allein’ werden nicht ausreichen, um genügend Bindung und Involvement zu erzielen – gerade im Rahmen von Change-Projekten wie Awareness-Kampagnen. Dies belegt z. B. der beinahe unsichtbare Erfolg von Beziehungsformaten wie Audio-Podcasts, denen gegenüber dem großen Bruder Video der Benefit inhärent ist, intime Verfassungs-Räume zu schaffen, bei denen man sich ohne visuelle Penetration hingeben und erlauben kann, mit sich und ein paar Stimmen, die einem sehr nahetreten und nahegehen, ganz Ohr sein zu dürfen, praktisch zu verschmelzen.

Sicher – selbst die wenigen, die mit dem täglichen Pendeln zur Arbeitsstätte bis vor kurzem noch eine gewisse erotische Komponente verbunden haben, mussten inzwischen feststellen, dass sich im Home Office bei entsprechend positiver Ausgangslage ohne Ablenkung konzentrierter arbeiten lässt. In diesem Kontext werden auch vermehrt Stimmen laut, dass man sich für eine „Rückkehr“ ins Unternehmen dann aus seiner heimischen Projektarbeit quasi frei nehmen muss, um den angestammten, betrieblichen Sozialraum erleben und mitgestalten zu dürfen. Eine verlängerte Distanz zur eigenen Organisation bei den Heimoffizieren lässt sich im neuen häuslichen Alltag also nicht leugnen.

Die aktive Suche nach einer Bindungs-Heimat im Unternehmen zeigt deutlich, dass Rückkanäle mit sozialer Zirkulation wertvoller sind als die Rezeption reiner Informationsbits aus dem Portal des sendefreundlichen Arbeitgebers. Um Beziehungen zu pflegen, sich face-to-face auszutauschen, nimmt man sich aus der Robinsonade einer heimeligen Projektarbeit mit Telkogelage Urlaub und sucht das „alte“ Büro als wärmendes Lage(r)feuer auf. Das Unternehmen wird dann – je nach Perspektive – Kneipe, Caféhaus, Vereinsheim, Kirche, Theater, Fußballstadion – mithin zum sozialen Couplingship. Aus dem digitalen Distanztanz mit Videokonferenz & Co. wird dann hier der soziale Con(s)tanz-Tee gefeiert.

Potenzielle Loser-Formate der Pandemie wie Face-to-face-Trainings, Workshops, Lernstationen, Events verkehren sich dann – in morphologischer Logik – zu sehnsüchtig erwarteten, postpandemischen Sozialpartys, weil die gemeinschaftshungrigen Robinson Cruisers seelische Durchbrüche, Selbstwirksamkeit, Kooperation, Einbindung u. a. soziale Benefits an ihren „alten“ Arbeitsplätzen erwarten. Vor allem diskursive Formate, die das „Talking-X“-Prinzip bedienen, schaffen die Voraussetzungen dafür, dass echte Kommunikation auf Augenhöhe mit Kollegen und Kolleginnen, bzw. Vorgesetzten unmittelbar ohne Technik-Vorspiel oder Video-Geplänkel auf allen Ebenen stattfinden kann: informell, non-. und, paraverbal.

Die erhöhte Nutzung von digitalen Formaten bzw. das Einlassen darauf führt zu einem seelischen Dilemma und steigert somit gleichsam die Sehnsucht nach sozialer Verbundenheit. Damit gekoppelt ist eine immense Erwartungshaltung gegenüber konkreten, sozialen Angeboten für den Fall regelmäßiger Teilhabe in und an den Organisationen – eben auch als Ausgleich zur einsamen Heimarbeit.

Daher ist die Implementierung von diskursiven Face-to-face-Formaten auf allen Ebenen – nicht nur im Kontext Information Security – wichtig und auch eine Chance in Bezug auf unternehmerische Sinnhaftigkeit (Purpose) und Weiterentwicklung – damit Titel wie „Stroke on the Water“ von „Deep Purpose“ nicht zum neuen Hitparadenflop in den Charts der Unternehmenskulturen geraten.

TAKE AWARE. TAKE AWAY. TAKE CARE.

Dietmar Pokoyski & Uwe Röniger, Herausgeber TAKE AWARE sec&life magazine

DAS SCHWEIGEN DER TRENNER

DAS „VERGESSEN“ VON SICHERHEITSMASSNAHMEN ALS FORM PASSIVER AGGRESSION UND VERMEIDUNG VON OFFENEN AUSEINANDERSETZUNGEN

von Dietmar Pokoyski

Sie kennen sicher diese Situation? Eine neue Policy, die mithilfe zahlreicher Awareness-Maßnahmen beworben und ausgerollt wird, weist zum x-ten Male auf den „richtigen“, d. h. erwünschten, Umgang mit Phishing-E-Mails hin. Jedoch ausgerechnet die vermeintlich „cleversten“ Kollegen und Kolleginnen fallen wieder einmal darauf rein, indem sie auf einen „verseuchten“ Link klicken und sich einen Trojaner einfangen. Abgesehen vom Beweis, dass Awareness mit Bildung wenig zu tun hat – ist das nun unter „Faulheit“ einzuordnen? Oder „schlechte Awareness“? Haben die unsere Regeln schlichtweg vergessen? Oder einfach nur Pech gehabt?

Die Antwort ist einfach, weil keine der oben angebotenen Erklärungen im Detail zutrifft, wird aber wieder kompliziert, wenn man derartige und ähnliche Fehler psychologisch erklären soll. „Wir haben doch alles richtig gemacht“, denkt dann vermutlich haareraufend der CISO. Und: „Keine Sicherheitsregeln sind umfassender durch alle Kanäle erklärt worden wie die zum Umgang mit E-Mails und dem Phishing-Risiko.“

Das Vergessen als Reaktanz

Um das so genannte „Vergessen“ im Kontext von Sicherheitsmaßnahmen und anderen Regularien zu erklären, lohnt nicht nur ein Rückblick auf unsere beinahe 20 Jahre alte, erste tiefenpsychologische Wirkungsanalyse über Fehlerkultur, „Entsicherung am Arbeitsplatz“ (Köln 2006), sondern auch eine „Neubewertung“ des Vergessens als „Kollateralschaden“ einer passiv-aggressiven Handlung. In der o. g. Studie haben wir die von uns beschriebene Reaktanz von Mitarbeitenden auf Sicherheitsmaßnahmen vertiefend analysiert. Diese Reaktanz möchte ich hier und heute aus dem Blickwinkel so genannter „passiv-aggressiver“ Motive vertiefen.

Beim Verstehen der Motive passiver Aggression helfen unter anderem die Bücher (u. a. „Vom Sinn des Ärgerns“), Vorträge bzw. Hörbücher der schweizerischen Psychologin Verena Kast*. Kast betrachtet passiv-aggressive Handlungen als Ärger im Sinne eines Nähe-Distanz-Reglers, jedoch in „eigentlich“ abgeschwächter Form. Die Einschränkung „eigentlich“ meint, dass der passive Anteil der Aggression unbewusst als unabsichtlich-absichtlicher Aggressionshemmer eingesetzt wird, damit die Sichtbarkeit des Ärgers vom Gegenüber, meiner Zielperson, moderater wahrgenommen wird als er eigentlich intendiert ist. Als Beispiele führt sie u. a. Gähnen, Flatulenzen, Schwitzen, Schweigen oder Vergessen an.

Gähnen, Furzen & Co. als nonverbale Aggression

Beim Gähnen in sozialen Konstellationen wird der Widerstand der gähnenden Person gegen das Hier und Jetzt deutlich, verbunden mit der „geheimen“ Botschaft „Ich will (eigentlich) ins Bett.“ Penetrante Blähungen sind, wenn man sie nicht eindeutigen medizinischen Ursachen zuschreiben kann und sie sogar einer gewissen Choreographie zu folgen scheinen (d. h. zum Beispiel paraverbal eingesetzt) Abwertungen von Kommunikationssituationen bzw. -partnern im Sinne von „Das, was hier läuft, ist ein doch ein Furz.“ In beiden oben beschriebenen Beispielen ist die passive Aggression an den Körper delegiert, in der Regel also unbewusst „gemacht“. Die Rechtfertigung lautet dann: „Das bin ja nicht ich, ätsch, denn ich kann das ja gar nicht kontrollieren.“ Gähnen und Fürze werden dann als aus dem Körper heraus fließend, als unkontrolliert wahrgenommen.

Jedoch können die Irritationen oder Missverständnisse, die ein derartiges Verhalten beim Gegenüber auslösen, durchaus von den Verursachern miteingepreist werden. Dann nämlich, wenn dieses „Sprechen“ des Körpers als Reaktion auf einer halbunbewussten Ebene geschieht, zum Beispiel in Situationen bei denen die Blähungen nach zustimmenden Personen im Raum suchen und somit quasi „ansteckend“ werden. Dann nämlich, wenn also die eigene Position durch weitere passiv-aggressiv furzende Mitstreiter gestärkt wird, indem das dann „heimlich“ miteinander verbundene Team praktisch im Chor Flatulenzen loslässt. Hierdurch kann man das Passiv-Aggressive in einer noch machtvolleren Position verorten als im Kontext einer gänzlich unbewussten Haltung.

Beim Schwitzen scheint die Aggression aus klassischer Konventionssicht stiller als beim Gähnen oder Furzen, wird aber dennoch ebenso machtvoll kundgetan. Denn Aggressionsschweiß nehmen wir in der Regel als unangenehmer, deutlich „ätzender“ wahr als zum Beispiel Angstschweiß, stets verbunden mit der Botschaft „Wie ätzend ist all‘ das, was ich hier gerade erlebe.“

Ein Schweigen – mehr als 1.000 Worte

Auch dem Schweigen oder Vergessen sind äußerst machtvolle Wirkungen inhärent. Mit permanentem Schweigen oder passiv-aggressivem Vergessen können wir unser soziales Umfeld regelrecht auf die

**Verena Kast, Jahrgang 1943, studierte Psychologie, Philosophie und Literatur und promovierte in Jungscher Psychologie. Sie war Professorin für Psychologie an der Universität Zürich, Dozentin und Lehranalytikerin am dortigen C.-G.-Jung-Institut und Psychotherapeutin in eigener Praxis. Von April 2014 bis März 2020 war sie Präsidentin des C.G. Jung-Instituts, Zürich, Küsnacht (Quelle: https://www.verena-kast.ch/)*

Palme bringen, indem wir unsere Verantwortung an andere delegieren. Gerade aus Sicht der Informationssicherheit sind beide passiv-aggressiven Strategien äußerst interessant, denn die Sicherheitsbereiche wollen ja in der Regel mutige und aktive Mitstreiter beim Schutz der Organisationsassets gewinnen, unter anderem mithilfe von wichtigen Regeln, die memoriert und praktisch angewendet werden sollen, um die Risiken zu senken bzw. die Compliance zu stärken. Mit Mitarbeitenden, die ihre Kollegen und Kolleginnen nicht grüßen, denen es in sozialen Situationen die Sprache verschlägt und die im Worst Case in eine totale Stummheit verfallen, ist Sicherheit ebenso wenig umsetzbar wie mit solchen, die ständig ihre Passwörter oder die sichernden Detailprozesse der Regelwerke „vergessen". Der Ärger der Kollegen und Kolleginnen wird dann umso größer, wenn diese bemerken, dass die Stummen und Vergesslichen außerhalb der Arbeit gegebenenfalls gänzlich abweichendes Verhalten zeigen und durchaus lebendig kommunizieren oder aber Sicherheitsregeln einhalten können. Verena Kast nennt dieses Phänomen „Selektivmutismus". Die Stummheit ist hier zum Beispiel passiv-aggressiver Ausdruck eines Unwohlseins im bestimmten Kontext bzw. in Verfassungen, in denen man sich unwohl fühlt, zum Beispiel in der eigenen Organisation. Stummheit oder Vergessen, sagt sie, wären auch Ausdruck einer sadomasochistischen Kollusion, also dem Zusammenspiel von zwei unterschiedlichen psychischen Dynamiken im Sinne von Interaktionsmustern: die eine fühlt sich unterlegen, die andere überlegen – beide haben dann was davon, so zu reagieren, wie es umgesetzt wird.

Wer vergessen wird, vergisst

Diese Konstellation beschreibt sehr prägnant ein uns bekanntes Machtgefüge in vielen hierarchisch angelegten Organisationen. Wenn wir nicht gehört werden, uns als Verlierer sozial-kommunikativer Konstellaltionen betrachten und infolge dieser Verluste Fatalismus entwickeln, neigen wir dazu, uns resignativ, passiv zurückzunehmen. Das Vergessen ist dann Teil einer situationsbedingten, unbewussten oder halbunbewussten passiv-aggressiven Strategie. Diese Strategie kennt vermutlich jeder von uns, denn es gibt keinen durchgängig passiv-aggressiven Typus – ein passiv-aggressives Interaktionsmuster ist stets an bestimmte Verfassungen gebunden, nicht prinzipiell an Menschen schlechthin. Wenn man vergisst, fühlt man sich in der damit gekoppelten Verfassung kontrolliert und neigt zur Abspaltung bzw. Delegation. Sicherheitsmaßnahmen müssen dann zum Beispiel „die anderen" situativ für einen selbst mitübernehmen. Eine derartige Haltung, eh nichts zu Sicherheitsmaßnahmen beitragen zu können, erleben wir häufig in Organisationen, die InfoSec vor allem aus technisch-prozessualer Perspektive betrachten und steuern bzw. dazu neigen, das Menschliche zu „vergessen". Im Umkehrschluss könnte man also behaupten: Wer vergessen wird, vergisst. Eben auch Sicherheitsregeln.

Mangelndes Selbstwertgefühl – Risiko für die InfoSec

Wie können aber Organisationen die unproduktiven Situationen passiver Aggressionen und den damit verbundenen Mangel des Selbstwertgefühls ihrer Mitarbeitenden überwinden? Ganz einfach: die Menschen miteinbeziehen und miteinander sprechen. Zum Beispiel darüber, wo wann bzw. bei welchen Gelegenheiten Sicherheitsmaßnahmen „vergessen" werden. Dabei müssen Sie genau hinschauen: Ist das Vergessen im Sinne eines oft bemühten Klischees „lediglich" Überforderung oder ist es – seriös gedacht – etwa Ausdruck einer passiven Aggression. In jedem Fall, so Kast, sollte das „Auftragswesen", mithin die Rolle der Mitarbeitenden und der Grad der Delegation, überprüft werden. Je stärker Organisationen Kanäle technisch-prozessual abdichten, je größer das Entmündigungsgefühl der Menschen, umso stärker das passiv-aggressive Potential mit einem deutlichen Risiko von „Vergessen" und potenziell damit verbundenen Security Incidents. Wenn man „vergisst", fühlt man sich kontrolliert und damit auch entwertet, d. h. man fühlt sich als „wertlos".

Und noch ein kontextuelles Detail, das die Nähe zur Informationssicherheit belegt: Passive Aggression ist persönliche Risikovermeidung, jedoch eine, die eben nicht zur Stärkung der InfoSec beiträgt. Im Gegenteil: eine passiv-aggressive Kommunikationskultur stellt ein hohes Sicherheitsrisiko dar. Wir sollten uns vielmehr „aktiv aggressiv" miteinander auseinandersetzen. Denn Ärger, der konstruktiv wirksam wird, macht zwar – „gute" wie „schlechte" – Emotionen spürbar, trägt aber eben auch zu Entwicklung und Selbstentfaltung von Individuen und Gemeinschaften bei. Wer seinem Ärger offen Luft verschafft, überwindet die Angst, der andere könnte hierauf ausschließlich negativ reagieren und lernt eben auch die eigenen Grenzen kennen, weiß wann die Situation eskalieren könnte und aus Aggressionen potenziell unproduktive Aggressionsketten werden. Eine offene Aussprache von Ärger fördert die Verbesserung der Kommunikation und somit auch das soziale Miteinander bzw. die Produktivität innerhalb einer Gemeinschaft. Reibung erzeugt Wärme.

Der Subtext macht die Botschaft

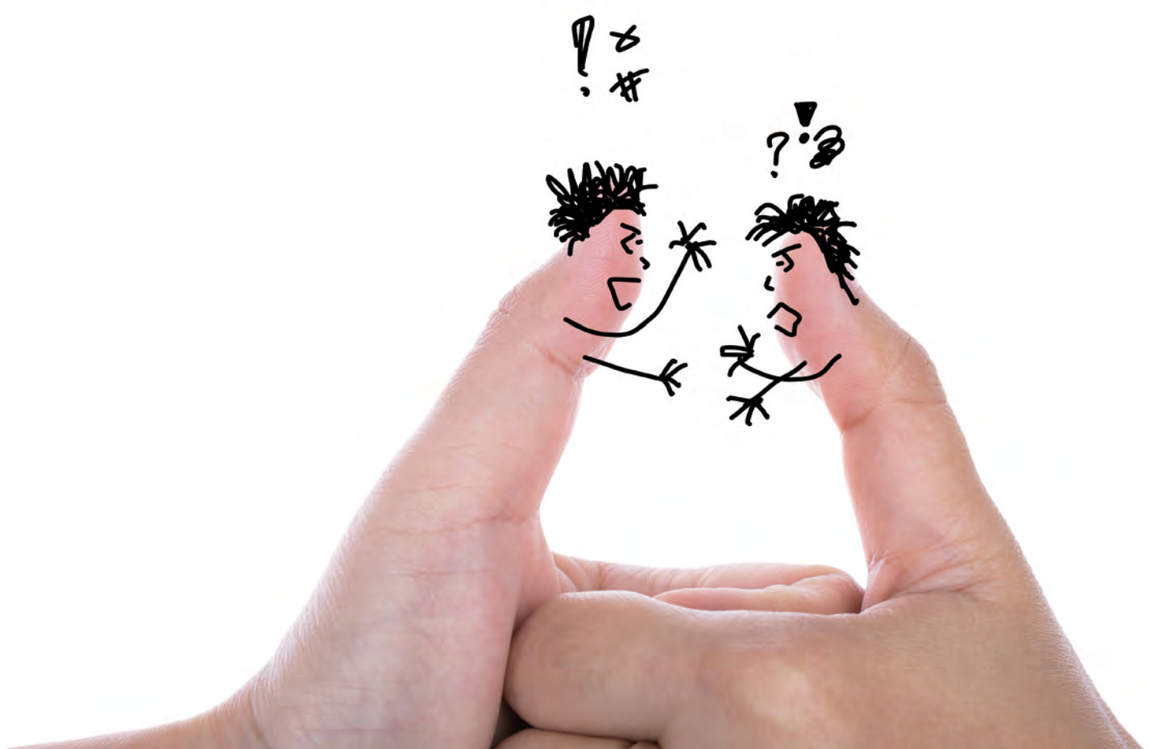
Miteinander reden oder – wenn das nicht so gut funktioniert – (paradoxe) Interventionen können dazu beitragen, aus dem Dilemma der oben beschriebenen Kollusion herauszufinden. Verena Kast beschreibt in diesem Kontext unter anderem eine erfolgreiche Intervention eines Mannes, der seiner Ehefrau damit konfrontierte, sichselbst in ein sehr teures Hotel zu verziehen für den Fall, dass sie erneut in eine ihm hinlänglich bekannte und unangenehm aufstossende Schweigephase verfallen sollte. Nach einiger Zeit war allein' das Kofferpacken ausreichend, um ihr passiv-aggressives Schweigen zu unterbrechen. Gerade das Bewusstwerden bzw. Sichtbarmachen von passiv-aggressivem Verhalten hilft dabei, einen drohenden Kommunikationsabbruch zu verhindern. Passive Aggression ist häufig Teil einer ungesunden Machtkonstellation – die Kehrseite ist die Ohnmacht, denn Machtzuwachs ist stets ein Ausschluss aus dem Wir. Ohne das Wir können auch die Sicherheitsprofis Organisationen nicht adäquat schützen.

Offene Auseinandersetzung – Verstärkung der Human Firewall

Wenn Sie also künftig Security Incidents in Ihrer Organisation auf Grundlage so genannter „menschlicher Fehlleistungen" analysieren, achten Sie stets auf den Subtext, die implizite, „versteckte" Ebene. Gerade das „Vergessen" kann auf Reaktanz beruhen und die damit verbundenen Widerstände könnten Ausdruck einer passiven Aggression sein, deren Ursache eben auch nicht unbedingt außerhalb der Organisation verortet werden muss. Denn wenn Fehler in Bezug auf Informationssicherheit passieren und die damit verbundene passiv-aggressive Reaktion auf Prozesse oder Kultur Ihrer Organisation zurückzuführen sind, sind Sie nicht machtlos, sondern können etwas dagegen unternehmen.

Kultur ist modellierbar. Lassen Sie die Menschen, die Informationssicherheit mit uns umsetzen und gegen Risiken verteidigen, nicht alleine. Versuchen Sie, die toxische Trennung von Macht und Ohnmacht zu überwinden. Awareness bedeutet stets das Einbeziehen von Kultur, eben auch systemisch bedingte Ängste zu überwinden und das manchmal Unangenehme in Organisationen zu thematisieren.

Durch das Ansprechen von zum Beispiel passiver Aggression als oft verständliches, aber im Zweifel eben „ungünstiges" Reaktionsmuster kann vor allem das wichtige Prinzip „Talking Security" produktiv umgesetzt werden. Denn gerade Diskurse darum, wer wann welchen Ärger zurückhält, – natürlich ohne Bloßstellung einzelner Personen – stärken den viel beschworenen menschlichen Faktor, das Selbstwertgefühl des Einzelnen innerhalb der Gemeinschaft und damit auch die auf die Organisationsmitglieder verteilte Defense-Idee einer „human centered" Information Security – die Mitarbeitenden als kooperierende Sicherheitskette einer Human Firewall.

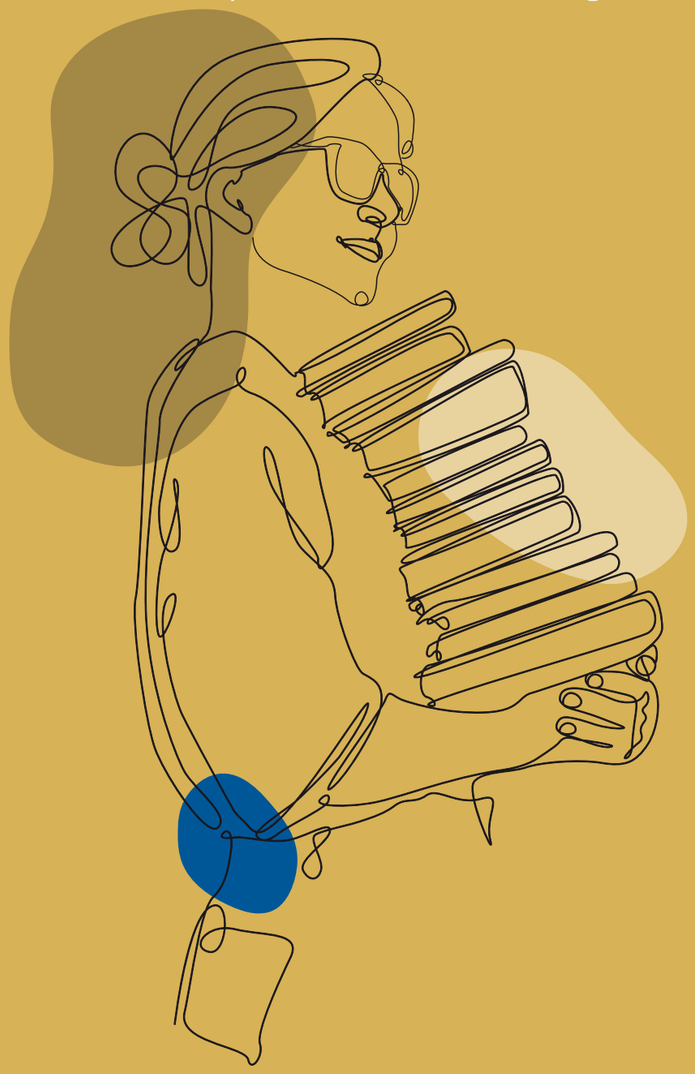


KLICKEN, LERNEN, HACKER STOPPEN

DIE SECURITY AWARENESS LIBRARY (SAL)

von Ulrich ten Eikelder, Deutsche Telekom Security
& Uwe Röniger, mybreev GmbH

Erhöhte Alarmbereitschaft in der Wirtschaft und in Behörden: Die Welle an Cyber Crime ebbt einfach nicht ab. Außerdem könnte der Ukraine-Krieg zu einem Cyber War eskalieren. IT-Kriminelle greifen inzwischen selbst Software-Konzerne an. Firewall und Virenschutz allein reichen nicht mehr – der letzte Abwehrwall ist die Belegschaft. Genau hier setzt die Security Awareness Library an – ein Video-Portal der Deutsche Telekom Security und von mybreev für professionelles E-Learning.



Security Officer, Firmeninhaber und Vorstände brauchen seit einiger Zeit Nerven wie Stahlseile: Im Internet rollt schier unaufhaltsam eine Welle an Cyberkriminalität. Vodafone Portugal , Kaseya , Solarwinds , die Software AG[1]. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rief Ende 2021 wegen der Java-Sicherheitslücke Log4 Shell die Alarmstufe Rot[2] aus.

Negativ-Rekord bei Cyber Crime

Und so könnte 2022 ein neues Negativ-Rekordjahr werden. Der deutsche Branchenverband Bitkom[3] konstatierte schon im August 2021 einen Schaden von 223 Milliarden Euro für die deutsche Wirtschaft – ein neuer Höchststand. Neun von zehn der mehr als 1.000 befragten Unternehmen (88 Prozent) waren demnach 2020/2021 von Angriffen betroffen. Und fast jedes zehnte Unternehmen (9 Prozent) sah sogar seine geschäftliche Existenz durch Cyberattacken bedroht.

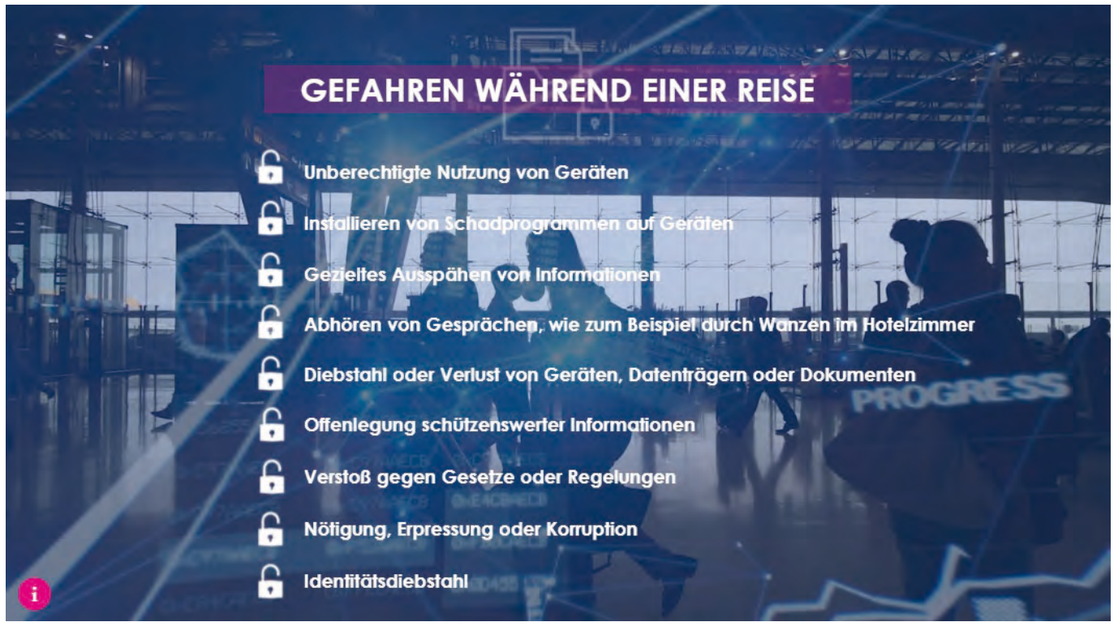
„Tatsächlich kann nur ein einziger falscher Click den Unterschied ausmachen zwischen geliefert haben und geliefert sein“, konstatiert Ulrich ten Eikelder, Head of Security Awareness and Communication bei der Deutsche Telekom Security GmbH. Und weiter: „Phishing, Social Engineering, CEO Fraud, Ransomware, DDoS-Attacken – das Arsenal der Hacker-Hölle ist gut gefüllt.“ Dazu gesellen sich die Bedrohungen in der Realwelt durch eigene Unachtsamkeit: vertrauliche Unterlagen offen auf dem Tisch, zu laute Telefonate, Interna in sozialen Netzwerken ausplaudern. Nachlässigkeiten, die viele Firmen plagen – weswegen die Telekom Security jetzt auch in den Markt expandiert.

Kooperation der Telekom Security und mybreev

Genau deswegen ist die Telekom Security eine Kooperation mit dem E-Learning-Anbieter mybreev eingegangen – das Ergebnis ist die Security Awareness Library. Sie bietet in gegenwärtig zehn interaktiven Video-Modulen das mentale Rüstzeug gegen Banditen, Industriespione und Innentäter. Die Länge der Module beträgt jeweils rund 15 bis 28 Minuten. Das vermittelte Wissen wird durch ein Quiz nochmals geprüft, um eine höhere Nachhaltigkeit und Verankerung zu erzeugen. Die E-Learning-Kurse bieten mehr als 200 Minuten interaktives und unterhaltsames Lernen mit realistischen Fallbeispielen aus dem Unternehmensalltag. Die digitale Bibliothek behandelt die Basics in Sachen Sicherheit: Phishing, Sicherheit auf Reisen und im Home Office oder Malware. Und vermittelt das Wissen für alles, was Angestellte gegen Angriffe von der dunklen Seite des Web und von der niederträchtigen Konkurrenz brauchen.

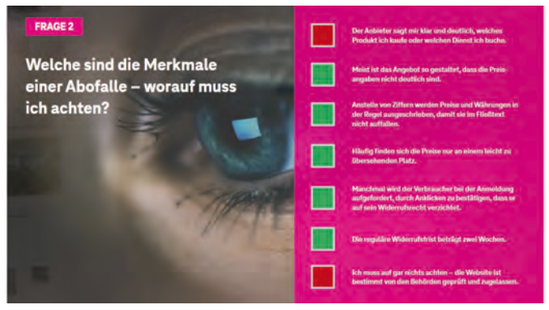
95 Prozent menschliches Versagen

„In der Wirtschaft tobt der Cyber-Darwinismus – nur die gut geschützten Firmen überleben“, urteilt auch Uwe Röniger, Geschäftsführer der mybreev GmbH. „Und neben der IT ist die Widerstandskraft von Kolleginnen und Kollegen der beste Schutz. Niemand sollte sich allein auf die Technik verlassen – sonst ist er oder sie verlassen.“ Zwar könne Achtsamkeit natürlich nicht vor professionellen



Kompromittierungen von Hackern gegen Sicherheitslücken in der Software helfen, erläutert Röniger weiter. Allerdings macht der Mensch durchaus den Unterschied: „IBM[4] hat schon 2014 gewarnt, dass 95 Prozent aller Sicherheitsvorfälle auf menschliches Fehlverhalten zurückgehen. Daran hat sich zu wenig geändert," ergänzt ten Eikelder.

Tatsächlich überlisten Cyber Gangster häufig Virenschutz und Firewall. Die Kriminellen werden immer professioneller, da auch die Abwehr immer ausgefeilter wird. Wenn die IT überwunden ist, entscheidet die Wachsamkeit bei Usern zwischen der Abwehr einer Attacke und dem Daten-GAU. Ergo kommt es auf die mentale Abwehrkraft von Mitarbeiterinnen und Mitarbeitern an – neudeutsch: Resilience. Besser nicht auf den Anhang in einer dubiosen Mail clicken. Lieber einen Entscheider um Rat fragen, wenn angeblich der Chef kurz vor dem Wochenende per Mail dringend eine Überweisung ins Ausland verlangt. Vertrauliche Dokumente niemals offen auf dem Schreibtisch liegen lassen.



Professionelles E-Learning im Netflix-Stil

„Hier setzen wir an mit der Security Awareness Library – wir schulen per Video-Storytelling und wollen so Wachsamkeit und Aufmerksamkeit praktisch vor Augen führen," erläutert Röniger weiter. Die E-Bibliothek deckt auf einer eigenen Website https://www.security-island.com/de/sal das komplette Repertoire für den Daten- und Informationsschutz ab. Mithilfe von realistischen Fallbeispielen und Quizelementen tauchen User ein in professionelle Video-Module. Immersiveness oder Immersivität nennen Experten diesen Zustand. Das Ziel ist spannendes Lernen mit Aha-Effekt im Netflix-Stil – aber ohne erhobenen Zeigefinger. Das Schlagwort ist Storytelling: Dadurch erreicht die Botschaft User über alle Hierarchieebenen hinweg – die Inhalte werden wirklich verstanden. Ein Konzept, das auch Pädagogen überzeugt: Die Security Awareness Library hat schon einen Comenius Award verliehen bekommen.

Die Security Awareness Library wird auch in der Deutschen Telekom global in aktuell vier Sprachen eingesetzt. Somit ist sie eine in der Praxis erprobte, ideale Ergänzung für die Stärkung der Security Awareness von Unternehmen. Für Firmen, die sich die Module einkaufen, bietet die Security Awareness Library noch andere positive Effekte: Sie sparen sich teure Unternehmensberater und Trainer, die eigenen Leute können dank der Internet-Anbindung lernen, wann immer und wo immer sie wollen. Und sie müssen keine Angst haben, sich mit Fragen vor den anderen im Team zu blamieren. Ein ganz besonderer Service ist die Individualisierbarkeit: Wer möchte, kann bei Bedarf sein spezielles Thema in seinem Stil in einem maßgeschneiderten Video verarbeiten lassen. Und sich somit quasi einen eigenen digitalen Ankerpunkt setzen in unruhigen Cyber-Zeiten.

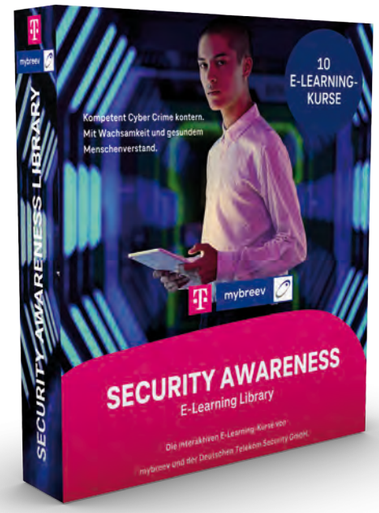
Fordern Sie Ihren persönlichen Testzugang an: www.security-island.com/de/sal

[1]https://www.heise.de/news/Terroristischer-Akt-Vodafone-Portugal-nach-Cyberattacke-komplett-ausgefallen-6364854.html
https://www.spiegel.de/netzwelt/web/kaseya-hack-von-70-millionen-dollar-auf-null-a-deeef8ef-f15f-4817-b69d-dcb474ce12f1
https://www.faz.net/aktuell/wirtschaft/digitec/solarwinds-hack-massiver-cyberangriff-gefaehrdet-deutsche-behoerden-17134477.html
https://www.handelsblatt.com/technik/it-internet/cyberkriminalitaet-832-gigabyte-daten-erbeutet-software-ag-arbeitet-die-juengste-hackerattacke-auf/26644250.html

[2]https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4Shell_WarnstufeRot.html

[3]https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

[4]https://www.securitymagazine.com/articles/85601-of-successful-security-attacks-are-the-result-of-human-error



CARE 4 AWARE

DER SECURITY AWARENESS-AWARD ZUM ZWEITEN

VON MICHAEL HELISCH & DIETMAR POKOYSKI

Zum zweiten Mal nach 2020 werden von den TAKE AWARE EVENTS in Zusammenarbeit mit HECOM Security Awareness Consulting und unter der Marke „CARE 4 AWARE“ die besten Security Awareness-Initiativen im deutschsprachigen Raum ausgezeichnet – diesmal für die Jahre 2020 bis 2022. Der Wettbewerb richtet sich sowohl an Unternehmen aus der Privatwirtschaft wie auch an öffentliche bzw. nicht-kommerzielle Träger, nicht aber an Dienstleister wie Agenturen, Beratungsunternehmen oder Anbieter von Tools. Die Prämierung der besten drei Wettbewerbseinreichungen (Shortlist) erfolgt durch eine Expertenjury (Ulrike Albanese & Stefano Merenda/Propella Design, Prof. Martina Sasse/RUB – Ruhr Universität Bochum, Frank Strebe/BMW, Kris Harms/Kommunikation, Training, Projektmanagement, Dr. Christoph Schog/Ex-T Systems International, Prof. Kristin Weber/ Hochschule Würzburg Schweinfurt).

Ausgeschrieben wurden drei Kategorien:

1. PROMOTE: Bestes Security Branding (Kombination der Kampagnenelemente Logo, Key Visuals, Logo, Claim, Naming, Wording etc.)

2. PERFORM: Beste (kurzfristige) Security Awareness-Kampagne

3. CHANGE: Bestes (mittel- bis langfristiges) Security Awareness-Programm

Da keine der Einreichungen die Anforderungen für „CHANGE“ erfüllt hat, wird für diese Kategorie in 2022 weder eine Shortlist, noch ein Gewinner ermittelt.

Die Texte auf den folgenden Seiten sind Auszüge aus den O-Tönen der jeweiligen Bewerbung.

Care4Aware: 1. PLatz in der Kategorie PROMOTE: Commerzbank AG: „Hacker Island – mit Sicherheit zu neuen Ufern “ (2020 ff.)

» Die Informationssicherheitskampagne soll sich so gut wie möglich aus der allgemeinen Informationsflut abheben, um eine höchstmögliche Wahrnehmbarkeit bei den Mitarbeiterinnen und Mitarbeitern zu erreichen. Unser Format erfüllt folgende für uns wesentlichen Anforderungen: neu und frisch, mit Humor, schnell – Leser muss nur wenig Zeit investieren, um einen Impuls zum Thema zu erhalten, Veröffentlichungen sprechen verschiedene Arten von Konsumenten an; daher besteht jede Episode aus: Comic, Goldene Regel (Kurzfassung), sachlicher Artikel, goldene Regeln (Langfassung), Narrativ tragfähig über die gesamte Zeit der Kampagne, Inhalte für jeden Leser nachvollziehbar und verständlich, international einsetzbar.

Auf Hacker Island gibt es sechs Hauptcharaktere: Die gute Seite: Käpt’n Safe, der leicht nerdige Kapitän des „myEyeboards“. Er möchte auf dem myEyeboard einen neuen Weltrekord aufstellen: die Weltumsurfung auf einem technisch hochgerüsteten Surfboard. Safe ist für jedes technische Gimmick zu haben, und dabei manchmal etwas unvorsichtig. Easy, Safes bester Freund, ist ein Papagei, der Safe aus manch brenzlicher Situation rettet und sich in Sachen Informationssicherheit gut auskennt. Das myEyeboard ist ein Surfboard, das fast alles kann. Die böse Seite: Bartholomew Ransomheart, der Chef des Hackerteams. Er möchte unbedingt die Pläne des myEyeboards erbeuten. Ann O’nymous ist die Computerspezialistin des Teams, Data Kraken sammelt mit seinen 6 Armen Daten – so viel und so oft wie möglich.

Die Namen sind auf beiden Seiten Programm. Sicherheit soll einfach sein (Safe & Easy), die Bedrohungen durch die „böse Seite“ sind allgegenwärtig und vielfältig. Die Umgebungswelt einer „Insel in der Südsee“ mit Piraten als Hacker ist relativ weit weg von einem klassischen Firmenumfeld – dies sorgt direkt für die gewollte Aufmerksamkeit, die zu Beginn in Einzelfällen sogar bis hin zur Irritation ging. Andererseits ist dieses Umfeld als Hintergrund für die geschilderten Abenteuer in einem quasi geschützten Raum für jeden Leser leicht nachvollziehbar (aus Filmen und Geschichten) und bietet viele Anknüpfungspunkte für kurze Erzählungen. Die in den Comics thematisierten Angriffe und Gegenmaßnahmen lassen sich dabei vom Leser sehr einfach auf das Firmen- oder Privatumfeld – also auf das „echte Leben“ - übertragen. Um den Wiedererkennungswert zu steigern, wurde in der internen Kommunikation hauptsächlich das Kampagnenlogo eingesetzt. Punktuell nutzen wir auch die Leitfigur oder – wenn passend – das Bild der Insel „Hacker Island“.

Die Kampagne wurde in zwei Staffeln veröffentlicht:
***Staffel 1:** 09.03.2020 – 09.03.2021, 24 Episoden*
(+2 Extra-Episoden zum Thema „Cloud Security”)
***Staffel 2:** 07.09.2021 – 22.02.2022, 12 Episoden«*

Care4Aware: 2. Platz in der Kategorie PROMOTE: EWE AG: „Mach sICHer möglich!“ (2021ff.)

»Unser Ziel ist es gewesen, einen Slogan zu entwickeln, der die Mitarbeitenden direkt anspricht und zum Handeln auffordert. Die Schreibweise und Satzstellung soll zum Nachdenken anregen und generell auf das Themenfeld aufmerksam machen. Durch „Mach sICHer möglich!“ wird der Mitarbeitende direkt angesprochen. Das „ICH“ wird im Satz visuell hervorgehoben, damit sich neben der Ansprache per Du und der Aufforderung durch das abschließende Ausrufezeichen der Mitarbeitende aufgefordert fühlt, zu handeln. Jeder Mitarbeitende selbst kann durch sICHeres Handeln zur Informationssicherheit beitragen. Das Logo wurde in allen Medien und Aktivitäten, die im Rahmen der Awareness-Kampagne erfolgten, eingesetzt. Dadurch standen alle Awareness-Aktivitäten im Kontext zu der Ich-Botschaft: „ICH kann sicher möglich machen“. Ein Widererkennungswert wurde geschaffen: Unsere Leitlinie für die gesamte Kampagne. Insgesamt wird das Logo neben den passenden Farben zum EWE CD mit einem gepunkteten Kreis abgerundet. Dieser soll sich nochmal schützend (mit Nachdruck) um die Worte legen.«

Care4Aware: 3. Plätze in den Kategorien PROMOTE und PERFORM GEA Group: „Security is my business. And yours“, „You are our first line of defense“ (2020 ff.)

»Unsere Ziele: allgemeine Awareness und Sensibilisierung für das Thema schaffen (z.B. Posterkampagne und Imagevideo), Stellenwert für Unternehmenserfolg und Dringlichkeit deutlich machen, ohne Ängste zu schüren, freundliche, aber verbindliche Tonalität.

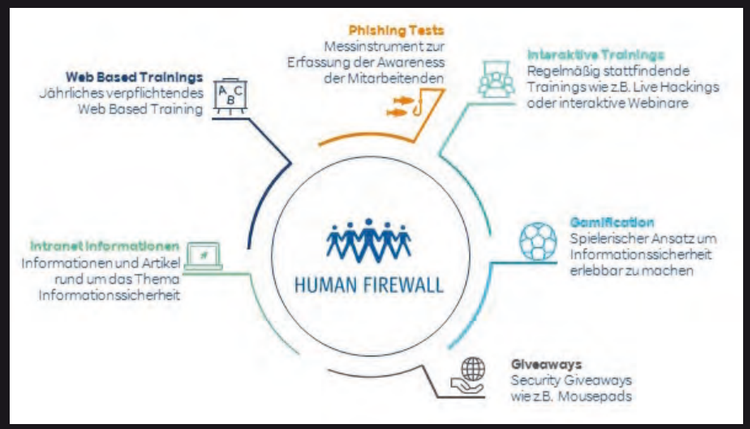
„You are our first line of defense“ – Sensibilisierung auf Handlungsebene, konkrete Beispiele unterhaltend präsentiert (Animationsvideos) und interaktiv erlebbar (z.B. Quiz), das technische, vermeidlich uninteressante Thema anhand von konkreten Fallbeispielen erfahrbar machen, Tipps für das alltägliche Handeln geben.

Signet: einprägsames Layout – Schloss als starkes und international gängiges Symbol für Schutz und Sicherheit, Netz steht für Digitalisierung, internationale Präsenz und Vernetzung – sowie die hieraus resultierende Verletzlichkeit der Informationen, Halbkreis / Schweif setzt Bezug zu GEA Logo.

Claim bzw. Slogan 2020: „Security is my business. And yours.“ Erweiterung 2021 um: „You are our first line of defense.“«.

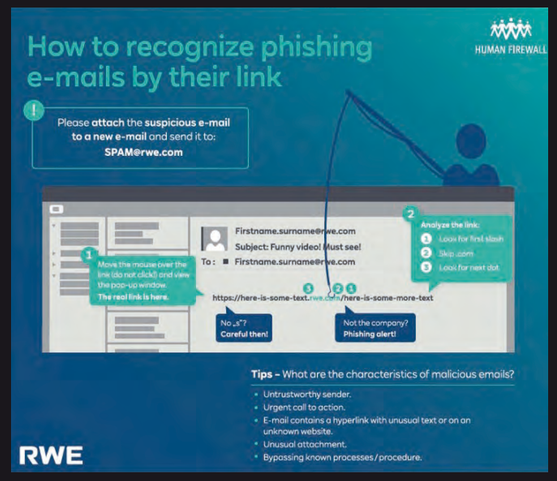
Deep-dive: Animationsvideos

Care4Aware: 2. Platz in der Kategorie PERFORM: RWE AG: „Human Firewa ll“ (2017 ff.)

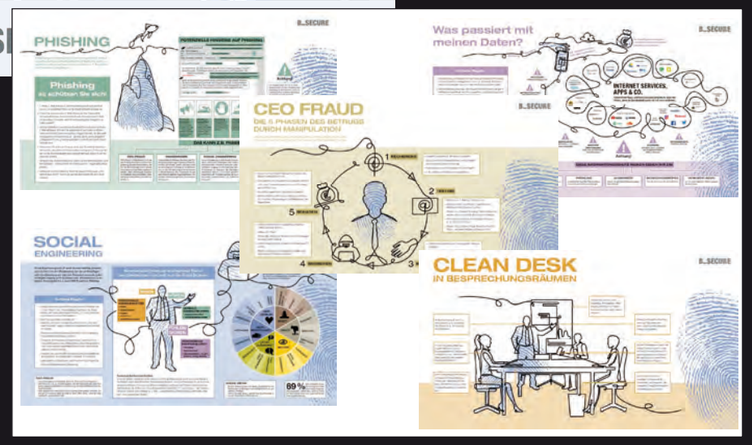


Das internationale Awareness Programm „Human Firewall“ des RWE Konzerns verfolgt seit 2017 einen ganzheitlichen Sensibilisierungsansatz, der relevante Schulungsinhalte für den dienstlichen und den privaten Alltag bietet, wichtig, da das Sicherheitsbewusstsein nicht am Drehkreuz des Unternehmens enden sollte, um Sicherheit in einer immer stärker digitalisierten Umgebung zu gewährleisten. Basierend auf diesem Vorgehen sind mehrere aufbauende Schulungsmodule entworfen worden. Jedes Jahr werden Cyber Security-Themenschwerpunkte fokussiert und in allen Maßnahmen mit aufgegriffen. Die Basis bildet das jährliche WBT, eine verpflichtende Online Schulung für alle Mitarbeitenden. Durch die automatische Unterstützung der HR-Systeme, erhalten alle neuen Mitarbeitenden bei RWE ein Security Paket mit Giveaways, einen Flyer mit den wichtigsten Themen in aller Kürze, sowie die verpflichtende Teilnahme am WBT zugestellt.

Aufbauend auf den WBTs werden regelmäßig Live Hackings als Präsenzveranstaltung durchgeführt. Abgerundet werden die Vorort Trainings durch zwei weitere Maßnahmen: Einen selbst entwickelten Cyber Escape Room und das Lernstationsformat „Security Arena“. Beide Maßnahmen behandeln auf spielerische Weise Security und erzeugen durch die Diskussion und Interaktion der Teilnehmenden ein nachhaltiges Erlebnis. Dies führt zu einer positiven Änderung des Verhalten hinsichtlich des Sicherheitsbewusstseins, da es sich um persönlich gesammelte Erfahrungen handelt. Darüber hinaus können Mitarbeitende sich über eine zentrale Themenseite im Intranet über relevante Security Fragen informieren und werden über Artikel im Intranet über aktuelle Sicherheitsthemen informiert. Außerdem unterstützt eine eigens entwickelte App bei der Klassifizierung und Handhabung von Informationen. Zur Ermittlung der Wirksamkeit aller Awareness Maßnahmen werden regelmäßig simulierte Phishing-Angriffen an alle Mitarbeitenden versendet und anonym ausgewertet. Die Ergebnisse werden genutzt, um vor allem während der Corona-pandemie interaktive Live-Trainings (sogenannte Websessions) zum Themen Phishing durchzuführen. Dazu wird eine Online-Plattform genutzt, auf der die Teilnehmenden aktiv mitwirken müssen, z. B. indem sie Fragen beantworten müssen. Der Trainer greift diese Ergebnisse auf und nutzt sie für die Diskussion mit den Teilnehmenden. Dadurch wird jedes dieser Trainings einzigartig, persönlich und vermittelt das nötige Grundfachwissen. Ein ganz wesentlicher Erfolgsfaktor für dieses Awareness Programm ist die Akzeptanz und die Unterstützung durch die RWE Vorstände. Es ist auch fester Bestandteil des Berichterstattung an den Vorstand, um die Entwicklung zu verfolgen und bei Bedarf Verbesserungsmaßnahmen zu beschließen.«



Care4Aware: 1. Platz in der Kategorie PERFORM: Bürkert Fluid Control Systems „B-Secure“ (2020ff.)



Die Kampagne umfasste zunächst den Zeitraum 2020-2022. Mitte/Ende 2020 wurde infolge von Corona die Entscheidung getroffen, bis auf Weiteres von Präsenzveranstaltungen und Vorort-Trainings auf „online“ umzuschwenken. Da die „Security Arena“ von known_sense als intensives Schlüsselmedium in der Kampagne ausgelegt war, ergab sich hieraus erstmal eine Hürde. Es wurden somit neue Medien benötigt, die es in wenigen Monaten abzustimmen und umzusetzen galt.

Mit dem neuen Medium „WBT“ wurde von der ursprünglichen Zielmaßgabe „Scope Deutschland“ abgesehen und direkt ein internationaler Rollout angesetzt. Dieser setzt sich in allen Medienformen durch: Poster, Lernkarten, Flow, Snapshot, Intranet, und WBT. Ebenso wurde aufgrund der WBTs der initiale Themenumfang von 3 auf 4 erweitert. Für die Themen 1 & 2, die bereits in 2020 begonnen wurden (aber in der Umsetzung teilweise ruhen mussten), wurden ebenso WBT-Module erstellt, sodass mit diesen in Q1 bzw. Q2 2021 gestartet werden konnte.

Zusammenfassend die Ziele/Projektumfang für 2021 Internationaler Rollout von 4 Themen-Blöcken:

- **Q1:** *Abschluss „Meine Informationen“ mit Intranet, Poster, Lernkarten, Snapshot, WBT, Webex-Schulungen*
- **Q2:** *Abschluss „Mein WWW“ mit Intranet, Poster, Lernkarten, Flow, Snapshot, WBT, Webex-Schulungen*
- **Q3:** *Abschluss „Meine E-Mails“ mit Intranet, Poster, Lernkarten, Snapshot, WBT, Webex-Schulungen*
- **Q4:** *Abschluss „Meine Trickser & Bluffer“ mit Intranet, Poster, Lernkarten, Flow, Snapshot, WBT, Webex-Schulungen*

Parallel dazu wurde in Q1-Q2 2021 eine Bürkert-weite E-Mail Phishing-Kampagne durchgeführt.«

B_SECURE

ALARM INFORMATIONSSICHERHEIT

von Prof. Dr. Margit Scholl

Typologie aus: Qualitative Wirkungsanalyse Security Awareness in KMU – tiefenpsychologische Grundlagenstudie im Projekt »ALARM Informationssicherheit«

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

Das Projekt

„ALARM Informationssicherheit“ baut innerhalb von drei Jahren ein Gesamtszenario zur Sensibilisierung und Unterstützung der KKU/KMU für Informationssicherheit bis hin zu deren Selbsthilfe auf. Im Projekt werden iterativ in drei Phasen, agil und partizipatorisch, ein innovatives Prozess-Szenario für Informationssicherheit mit analogen und digitalen erlebnisorientierten Szenarien sowie „Vor-Ort-Angriffen“ und weiteren Überprüfungen, wie z. B. Awareness-Messungen, Quiz und Tests entwickelt. Das Gesamtszenario soll zu der dringend notwendigen Sensibilisierung von Führungskräften und Mitarbeitenden und zu einer gezielten Personalentwicklung in KMU/KKU führen, wie sie derzeit breitenwirksam noch nicht vorhanden ist. Dazu wird IT-Sicherheit im Zusammenhang mit den zunehmend digitalen Arbeitsprozessen konkret (be-)greifbar gemacht, gleichzeitig werden die Menschen emotional berührt und aktiv in die Entwicklung von Maßnahmen einbezogen. Eine nachhaltige und unternehmensweite Informationssicherheitskultur soll damit aufgebaut werden.

Ziele und Inhalte

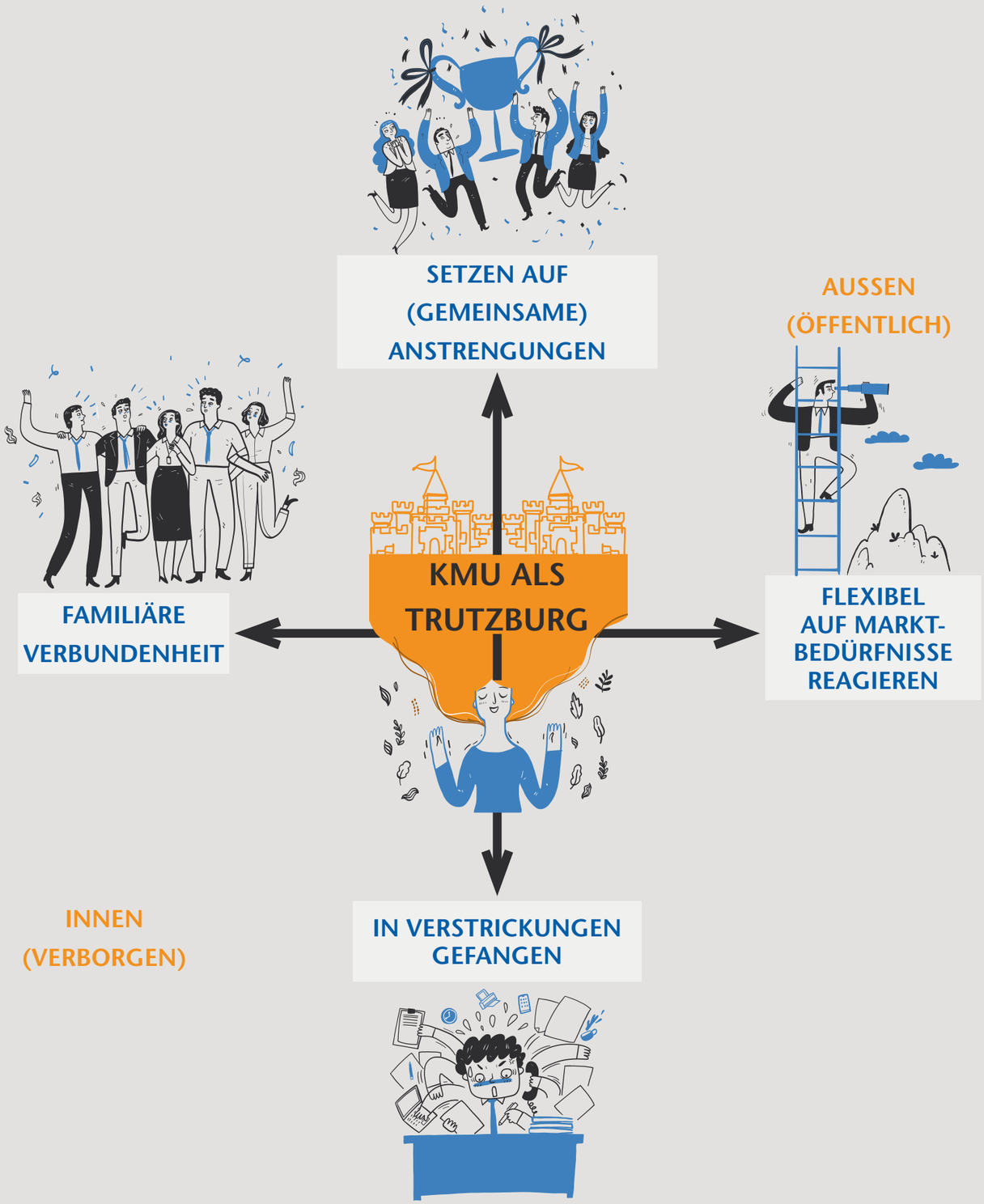
Es werden Defizitbereiche wichtiger Geschäftsprozesse systematisch und gemeinsam mit Pilot-KMU und -Handwerksbetrieben anhand konkreter Tätigkeiten erschlossen und Sicherheits- sowie Kompetenzprofile abgeleitet. Um Nachhaltigkeit auch breitenwirksam zu erreichen, werden aktivierende Sensibilisierungsmaßnahmen analog und digital entwickelt, praktisch vielfältig erprobt und evaluiert. Best-Practice-Anleitungen mit Erfolgsgeschichten teilnehmender Unternehmen werden bundesweit über assoziierte Transferpartner veröffentlicht, um weitere Unternehmen anzusprechen. Neuartige betriebliche Awareness-Messungen führen zu Reifegradaussagen für KMU/KKU. Qualitäts- und Ergebnissicherung kombiniert mit Risikomanagement und einer begleitenden Evaluation komplementieren die Wirkungsanalysen. Die Vernetzung aller Beteiligten wird bundesweit verstärkt.

Methoden

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

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

PSYCHOLOGISCHE KONSTRUKTION DER SICHERHEITSKULTUR IN KMU



Aus: Qualitative Wirkungsanalyse Security Awareness in KMU – tiefenpsychologische Grundlagenstudie im Projekt »ALARM Informationssicherheit«

Qualitative Wirkungsanalyse Security Awareness in KMU – tiefenpsychologische Grundlagenstudie im Projekt »ALARM Informationssicherheit«, Wildau, 2021. ISBN 978-3-949639-00-5

Führungskräfte und Mitarbeitende sehen sich stolz als Team mit hoher Identifikation und engen Bindungen in ihrem kleinen und mittelgroßen Unternehmen. Doch wie sieht es mit der Informationssicherheit (information security) und dem entsprechenden Bewusstsein (awareness) in deutschen KMU bzw. KKU aus? Diese tiefenpsychologische Grundlagenstudie verdeutlicht den Ist-Stand und will gleichzeitig mit ihren Empfehlungen einen Mehrwert für KMU aufzeigen.

Die Studie offenbart, dass der Begriff Informationssicherheit für viele noch diffus ist und nicht selten Experten und Dienstleistern zugeordnet wird. Zukünftig sollte daher die persönliche Wahrnehmung auf die eigene Verantwortung für Informationssicherheit am Arbeitsplatz geschärft werden. Zudem verdeutlichen die von den Interviewten genannten relevanten Themen, dass der Awareness-Reifegrad noch deutlich ausgebaut werden kann, denn auf den ersten beiden Plätzen liegen die altbekannten Problemfelder Passwortsicherheit und Phishing-Attacken. Damit wird deutlich, dass in KMU verstärkt für alle eine Bewusstseinsbildung (awareness raising) für Informationssicherheit stattfinden sollte.

Ganzheitliche Awareness-Konzepte, wie im vom BMWi/BMWK geförderten Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ vorgesehen, oder ein Awareness-Rahmenprogramm mit dokumentierter Strategie kommen bisher in den befragten KMU nicht zum Einsatz. Aktivitäten für mehr Awareness werden bislang oft nur in Form einer reinen Wissensvermittlung verstanden - das greift zu kurz. Lesen Sie dazu die Studie auf Deutsch.

https://alarm.wildau.biz/
https://doi.org/10.13140/RG.2.2.21236.88961

Report zur Informationssicherheit in KMU – sicherheitsrelevante Tätigkeitsprofile. Wildau, 2022. ISBN 978-3-949639-01-2

Auch die Ergebnisse unserer ersten Online-Umfrage innerhalb des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“ lassen vermuten, dass Informationssicherheit nicht in allen KMU tatsächlich ganzheitlich wahrgenommen wird.

Der Report gibt einen konkreten Einblick in die Ist-Situation von KMU unter Pandemie-Bedingungen in 2021, um aus Tätigkeitsprofilen mit Hilfe des IT-Grundschutzes des BSI entsprechende Sicherheits- bzw. Kompetenzprofile abzuleiten.

Es werden dazu die folgenden Tätigkeitsfelder untersucht:

- Tätigkeitsfeld „Fertigung/Produktion“
- Tätigkeitsfeld „Materialwirtschaft/Logistik/Lager“
- Tätigkeitsfeld „Einkauf und Beschaffung“
- Tätigkeitsfeld „Vertrieb/Außendienst“
- Tätigkeitsfeld „Kundenmanagement/Kundenservice“
- Tätigkeitsfeld „Prozessmanagement/Qualität/Controlling“
- Tätigkeitsfeld „Forschung/Entwicklung“
- Tätigkeitsfeld „IT/Administration“
- Tätigkeitsfeld „Sekretariat/Empfang/Pförtnerei/Poststelle“
- Tätigkeitsfeld „Finanzen/Buchhaltung/Rechnungswesen“

Außerdem werden folgende Personengruppen näher beleuchtet:

- Personengruppe „Geschäftsleitung/Top-Management“
- Personengruppe „Mittleres Management“
- Personengruppe „Mitarbeitende“
- Personengruppe „Auszubildende/Praktikanten“.

Der Report steht ab Mai 2022 auf der Projektwebseite auf Deutsch zum Download bereit https://alarm.wildau.biz/

WIE VERMITTELT MAN CYBER-SICHERHEIT?

AWARENESS-MASSNAHMEN DES BUNDESAMTS FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

von Karin Wilhelm und Angelika Jaschob

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfolgt im Rahmen seines Digitalen Verbraucherschutzes unter anderem das Ziel, das Risikobewusstsein von Verbraucherinnen und Verbrauchern zu erhöhen. Die Menschen sollen sich klar darüber sein, was sie im Falle eines Cyber-Vorfalls verlieren könnten. Darüber hinaus will das BSI die Lösungskompetenz von Verbraucherinnen und Verbrauchern steigern. Die Menschen sollen wissen, wie sie bei einem IT-Notfall reagieren. Es gibt eine Reihe von Informationen und Empfehlungen des BSI zur Cyber-Sicherheit. Doch wie können diese Inhalte so aufbereitet und verbreitet werden, dass sie im digitalen Alltag der Verbraucherinnen und Verbraucher ihren Einsatz finden?

Digitalbarometer

Um die Informationsbedürfnisse der Menschen zu verstehen, führt das BSI gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) eine repräsentative Online-Befragung durch, das Digitalbarometer. Die Ergebnisse aus 2021 zeigen, dass nur 15 Prozent der Befragten sich regelmäßig zu Cyber-Sicherheit informieren, 22 Prozent sogar nie. Die meisten beschäftigen sich nur hin und wieder oder erst im Problemfall – wenn es möglicherweise zu spät ist – mit dem Thema Informationssicherheit. Häufig fehlt es somit an einem grundsätzlichen Interesse.

Webseiten und Newsletter

Zu den wichtigsten Informationsquellen gehören Webseiten und E-Mail-Newsletter – etwa zwei Drittel der Befragten informieren sich dort zu Schwachstellen und Empfehlungen. Deswegen bilden diese Elemente auch einen wichtigen Teil der Awareness-Arbeit des BSI. Die Webseite bsi.bund.de bietet unter anderem konkrete Handlungsempfehlungen zu Fragen des digitalen Alltags, liefert Hintergrundinformationen aus dem Bereich Cyber-Sicherheit und erreicht über Suchanfragen zahlreiche Menschen, die das BSI noch nicht kennen. 2021 stand sie beispielsweise für 160 Begriffe in Suchmaschinen auf Platz 1. Alle zwei Wochen erscheint der Newsletter „Sicher • informiert“ und hält über 120.000 Abonnentinnen und Abonnenten auf dem Laufenden zu aktuellen Entwicklungen der digitalen Welt.

Video-Formate und Podcast

Auf die Frage, wie sich die Teilnehmenden der Befragung zukünftig informieren wollen, werden neben der Webseite und dem Newsletter auch noch weitere Kanäle und Formate genannt: soziale Medien (20 %), (Erklär-)Videos (13 %), Apps (12 %) und Podcasts (10 %). Aus diesem Grund setzt das BSI auf einen Formate-Mix. Es ist sowohl präsent in den sozialen Medien, entwickelt regelmäßig neue Video-Formate und bietet seit über einem Jahr u. a. den Podcast „Update verfügbar“ an, der monatlich im Schnitt um die 5.000 Zuhörerinnen und Zuhörer hat.

Cyber-Sicherheitsnetzwerk

Ein zusätzliches Angebot für Verbraucherinnen und Verbraucher pilotiert das BSI gerade mit dem Cyber-Sicherheitsnetzwerk (CSN). Das ist ein freiwilliger Zusammenschluss von qualifizierten Helferinnen und Helfern, die ihre Expertise und ihr Know-how zur Behebung von IT-Sicherheitsvorfällen zur Verfügung stellen. Das CSN soll besonders für Verbraucherinnen und Verbraucher eine wertvolle Unterstützung bei einem IT-Sicherheitsvorfall darstellen. Zugleich bietet das Netzwerk zahlreiche Angebote, um sich auf einen Vorfall vorzubereiten und im Worst Case handlungsfähig zu sein.

Aber: Was ist, wenn die IT-Sicherheitsmaßnahmen nicht ausreichen?

Wenn die eigene IT trotz vorkehrender Sicherheitsmaßnahmen von einem IT-Sicherheitsvorfall betroffen ist, können Digitale Ersthelfer des CSN bei der Bearbeitung des IT-Sicherheitsvorfalls unterstützen. Je nach Vorfall stellt sich die Frage: Wer kann wie helfen? Das CSN hat hierfür die „Digitale Rettungskette“ entwickelt. Dort ist festgelegt, wer an welcher Stelle des Prozesses welche Aufgabe übernimmt. Die „Digitale Rettungskette“ reicht von der Unterstützung durch Checklisten über eine telefonische Beratung durch das CSN bis hin zu einem Team von Vorfalls-Experten, die vor Ort tätig werden können. Das CSN bringt mit der Digitalen Rettungskette qualifizierte Helferinnen und Helfer zusammen, die bei einem Vorfall koordiniert agieren können.

Auch IT-affine Personen können sich im Cyber-Sicherheitsnetzwerk engagieren und sich selbst zum Digitalen Ersthelfer qualifizieren lassen. Ein kostenloser Online-Kurs bietet den Einstieg in das Qualifizierungsprogramm des CSN. Nach Abschluss des Programms sind die Teilnehmenden in der Lage, kleine IT-Störungen und IT-Sicherheitsvorfälle strukturiert zu bearbeiten und Betroffene schnell und effektiv zu unterstützen. Der „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“ gibt den Rahmen der Vorfallsbearbeitung vor. Die Webseiten des CSN bieten eine schnelle Übersicht über diese regionalen qualifizierten Digitalen Ersthelfer.

Trainingskoffer mit Übungen und Spielen

Als Begleitmaterial stellt das CSN einen Trainingskoffer mit einer kostenfreien Übungs- bzw. Spielesammlung zur Verfügung. So wird ein spielerisches

Training der Vorfallsbearbeitung in einer vertrauensvollen Umgebung geschaffen. Alle Trainingseinheiten lassen sich ohne großen Aufwand einsetzen. Der Trainingskoffer ist modular aufgebaut und lässt sich sowohl durch die Forenleitung als auch durch Trainerinnen und Trainer oder andere Teilnehmende kontinuierlich um Spiele erweitern.

Nutzen Sie die BSI-Produkte für Ihren Awareness-Maßnahmen, in Schulungen oder Veranstaltungen!

Rettungskette
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210927_Digitale_Rettungskette.html

CSN
www.cyber-sicherheitsnetzwerk.de

Digitalbarometer 2021
https://www.bsi.bund.de/dok/974882

Verbraucher
www.bsi.bund.de/VerbraucherInnen du/

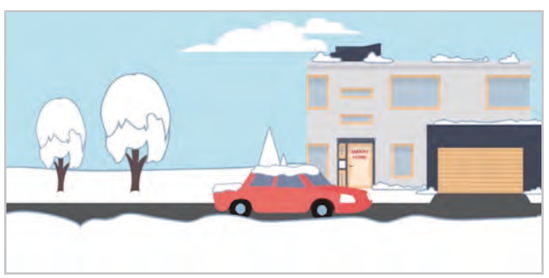
Lagebild
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.html

ACS
https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html

Unterschiedliche Formate des BSI für Verbraucherinnen und Verbraucher im Überblick

Newsletter: Der Newsletter „Sicher • Informiert“ richtet sich an alle, die über die wichtigsten Ereignisse rund um die Sicherheit ihres Computers und im Internet auf dem Laufenden gehalten werden wollen. Er erscheint alle vierzehn Tage.

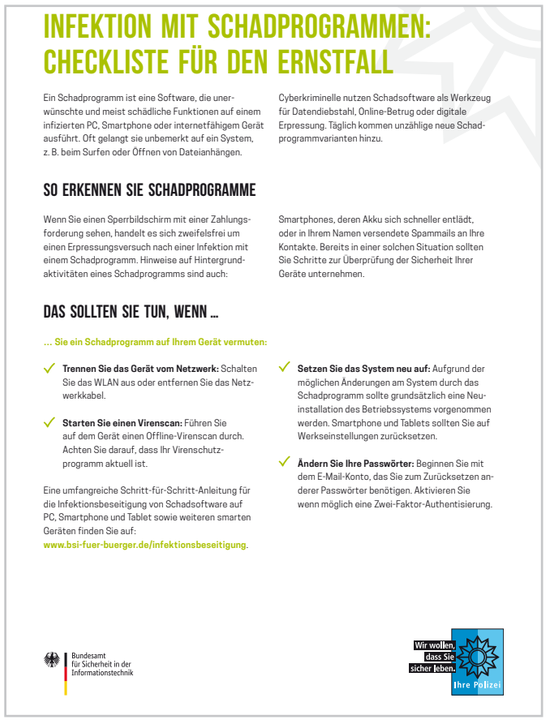
Podcast: Seit September 2020 informiert der Podcast „Update verfügbar“ Privatanwenderinnen und Privatanwender über Cyber-Vorfälle, Innovationen, skurrile Fakten und gibt hilfreiche Tipps.



Videos: Wie mache ich mein Smarthome sicher? Wie schütze ich mein Handy? Warum brauche ich Updates? In Animationsfilmen und Videos mit Expertinnen und Experten gibt es Tipps für den digitalen Alltag.

Broschüren: Die Wegweiser für den digitalen Alltag informieren über den sicheren Umgang im digitalen Alltag und bieten praxisnahe und hilfreiche Tipps zur IT-Sicherheit. Bestellbar oder zum Download auf der Website.

Checklisten: Was kann ich tun, wenn ich mir ein Schadprogramm eingefangen habe oder ich auf eine Phishing-Mail reingefallen bin? Die Checklisten für den Ernstfall helfen Ihnen Schritt für Schritt weiter.



INFEKTION MIT SCHADPROGRAMMEN: CHECKLISTE FÜR DEN ERNSTFALL

Ein Schadprogramm ist eine Software, die unerwünschte und meist schädliche Funktionen auf einem infizierten PC, Smartphone oder internetfähigem Gerät ausführt. Oft gelangt sie unbemerkt auf ein System, z. B. beim Surfen oder Öffnen von Dateianhängen.

Cyberkriminelle nutzen Schadsoftware als Werkzeug für Datendiebstahl, Online-Betrug oder digitale Erpressung. Täglich kommen unzählige neue Schadprogrammvarianten hinzu.

SO ERKENNEN SIE SCHADPROGRAMME

Wenn Sie einen Sperrbildschirm mit einer Zahlungsforderung sehen, handelt es sich zweifelsfrei um einen Erpressungsversuch nach einer Infektion mit einem Schadprogramm. Hinweise auf Hintergrundaktivitäten eines Schadprogramms sind auch:

Smartphones, deren Akku sich schneller entlädt, oder in Ihrem Namen versendete Spammails an Ihre Kontakte. Bereits in einer solchen Situation sollten Sie Schritte zur Überprüfung der Sicherheit Ihrer Geräte unternehmen.

DAS SOLLTEN SIE TUN, WENN …

… Sie ein Schadprogramm auf Ihrem Gerät vermuten:

- **Trennen Sie das Gerät vom Netzwerk:** Schalten Sie das WLAN aus oder entfernen Sie das Netzwerkkabel.
- **Starten Sie einen Virenscan:** Führen Sie auf dem Gerät einen Offline-Virenscan durch. Achten Sie darauf, dass Ihr Virenschutzprogramm aktuell ist.
- **Setzen Sie das System neu auf:** Aufgrund der möglichen Änderungen am System durch das Schadprogramm sollte grundsätzlich eine Neuinstallation des Betriebssystems vorgenommen werden. Smartphone und Tablets sollten Sie auf Werkseinstellungen zurücksetzen.
- **Ändern Sie Ihre Passwörter:** Beginnen Sie mit dem E-Mail-Konto, das Sie zum Zurücksetzen anderer Passwörter benötigen. Aktivieren Sie wenn möglich eine Zwei-Faktor-Authentisierung.

Eine umfangreiche Schritt-für-Schritt-Anleitung für die Infektionsbeseitigung von Schadsoftware auf PC, Smartphone und Tablet sowie weiteren smarten Geräten finden Sie auf:
www.bsi-fuer-buerger.de/infektionsbeseitigung.

Bundesamt für Sicherheit in der Informationstechnik

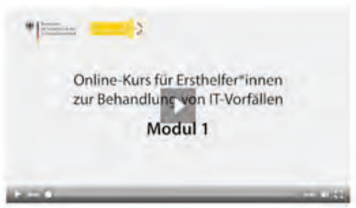
Wir wollen, dass Sie sicher leben. Ihre Polizei

Cyberfibel: 250-seitiges, leicht verständliches Handbuch für Vermittlerinnen und Vermittler, um Basiswissen und Digitalkompetenzen rund um die Cyber-Sicherheit weiterzugeben. www.cyberfibel.de

Recap-Video: Das 90-sekündige Video vermittelt in einen ersten Eindruck vom Cyber-Sicherheitsnetzwerk.

Erste Hilfe nach einem IT-Sicherheitsvorfall: Die Broschüre „Die Digitale Rettungskette des Cyber-Sicherheitsnetzwerks“ erklärt den Ablauf der Unterstützungsleitung bei der Vorfallsbehandlung im Cyber-Sicherheitsnetzwerk. Über die kostenfreie Hotline-Nummer 0800-274 1000 erhalten Betroffene Hilfe, ihren IT-Sicherheitsvorfall richtig einzuschätzen und am richtigen Glied der Digitalen Rettungskette einzusteigen.

Online-Kurs: Ein Basiskurs für Digitale Ersthelfer ermöglicht es, sich im kostenlosen Selbststudium zum Digitalen Ersthelfer zu qualifizieren und im CSN aktiv mitzuarbeiten.



Informationsgrafiken: DIN A3 Poster unterstützen die Arbeit des Digitalen Ersthelfers bei der Bearbeitung von kleinen IT-Störungen und kleinen IT-Sicherheitsvorfällen mit ersten Handlungsempfehlungen durch eine schnelle Übersicht.

Trainingssammlung: Der Trainingskoffer (Abb. s. S. 22) bietet mit seinen Spielen (Abb. hier „PROTECT & HACK“) eine interaktive Möglichkeit, sich mit dem Thema IT-Sicherheit und Vorfallbehandlung zu beschäftigen.

Postkarten: Die Postkarte bietet die Möglichkeit, Betroffene mit persönlichen Texten direkt anzusprechen .

Smishing

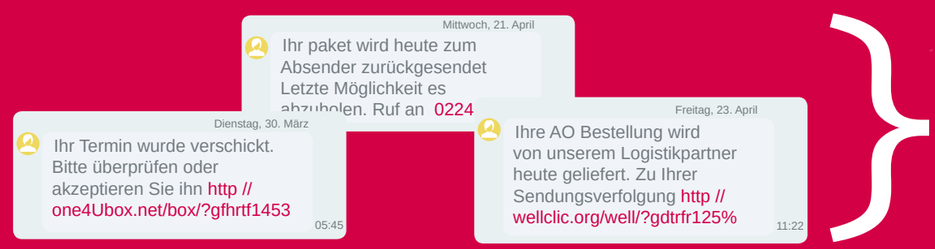
known_sense

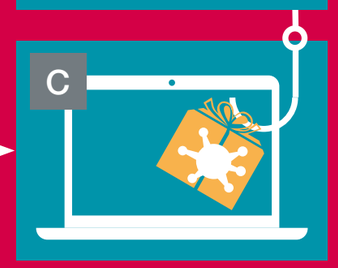
awareness you can touch.

3 Bei A) und B) besteht das Risiko, dass Sie ggf. sensible Informationen direkt an die Täter preisgeben.

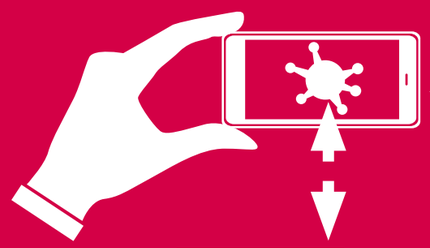
1 Cyberkriminelle senden eine Textnachricht, der Sie unter Vortäuschung dringenden Handlungsbedarfs dazu auffordert, auf einen Link zu klicken oder eine Nummer anzurufen.

2 Sie werden dazu aufgefordert,
- A) eine Hotline anzurufen und sich zu verifizieren
- B) oder Informationen in eine Eingabemaske einzutragen
- C) oder einen Download auszuführen.





3 Bei C) installiert sich als App getarnte Schadsoftware auf Ihrem Smartphone.



4 Schadsoftware liest Ihre Daten aus und übermittelt diese an die Täter, die damit ggf. Zugänge zu Ihren Anwendungen bzw. Konten erhalten.

5 Schadsoftware versendet massenhaft personalisierte Nachrichten an Personen aus Ihrem Adressbuch oder ruft diese an.

6 Ihre Kontakte werden ebenfalls infiziert und das Schneeballsystem wird kontinuierlich fortgesetzt.

- **Dies können Vorwände für Kontaktaufnahme von Cyber-Kriminellen sein:**
- Logistik: Sie sollen eine angeblich bestellt Sendung akzeptieren oder empfangen.
- Geldinstitut: Ihre Bank meldet „ungewöhnliche“ Aktivitäten auf Ihrem Konto.
- Online: Ein Web-Service bestätigt die potenzielle Eröffnung eines Premiumkontos o. ä.
- Kommunikation: Ihr Telefonanbieter erhebt zusätzliche Gebühren für potenzielle Extras.
- Boni & Gewinnspiele: Es werden Vergütungen oder Preise in Aussicht gestellt.
- Mahnungen: Sie werden beschuldigt, Zahlungen nicht ausgeführt zu haben.
- Termine & Ticketing: Ihre Termine (Event, Click & Meet, Impfzentrum, Arzt etc.) verschieben sich oder sollen bestätigt werden.
- etc.

UNSERE AUTOREN

***Ulrich ten Eikelder**, mit über 20 Jahre Erfahrung in der Security als verantwortlicher Leiter verschiedenster Fachteams auf Konzernebene ist Ulrich ten Eikelder auch extern ein anerkannter Experte. Als Dipl.-Ing. der Elektrotechnik zog es ihn früh zu eher kommunikativen Aufgabengebieten des Marketings und der Kommunikation. Zu seinen beruflichen Stationen zählen u.a. Auslandseinsätze für die Deutsche Telekom und die Teilnahme am Sicherheitspolitischen Seminar 2012 der Bundesakademie für Sicherheitspolitik. Seit 2014 leitet Ulrich ten Eikelder das Team der Security Awareness bei der Telekom Security.*

***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 Care 4 Aware hat er als Schirmherr gemeinsam mit den TAKE AWARE EVENTS aus der Taufe gehoben.*

***Angelika Jaschob**, Diplom-Mathematikerin, ist seit 1994 im Bundesamt für Sicherheit in der Informationstechnik (BSI) auf dem Gebiet der IT-Sicherheit tätig. Ihr erster Arbeitsschwerpunkt lag im Bereich der Kryptologie. Danach war sie in unterschiedlichsten Arbeitsgebieten der Zertifizierung und des IT-Grundschutzes tätig. Sie konzipierte und leitete mehrere Jahre Qualifikationsmaßnahmen für IT-Sicherheitsbeauftragte, Auditoren, Penetrationstester und Vorfall-Experten. Heute ist Frau Jaschob Projektleiterin des Cyber-Sicherheitsnetzwerks (CSN), welches das Ziel verfolgt eine flächendeckende dezentrale Struktur aufzubauen, über die kleine und mittlere Unternehmen, Bürgerinnen und Bürger bei IT- Sicherheitsvorfällen effiziente Unterstützung erhalten können. Mit dem Trainingskoffer stellt das CSN ein Hilfsmittel bereit, um die Themen der Digitalen Rettungskette bzw. der Vorfallbearbeitung spielerisch in einem Team zu trainieren.*

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

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

***Margit Scholl**, Professorin seit 1994, forschungsaktive Professorin für Wirtschafts- und Verwaltungsinformatik an der TH Wildau seit 1997, Leiterin des Labors für medienintegrierende Verwaltungsinformatik an der TH Wildau seit 2001, Gründung und Leitung des Wildau Instituts für innovative Lehre, lebenslanges Lernen und gestaltende Evaluation (WILLE) im Technologietransfer- und Weiterbildungszentrum (TWZ) an der Technischen Hochschule Wildau e.V. seit 2010, Qualifizierungsstelle der Bundesakademie öffentliche Verwaltung (BAköV) seit 2010, seit 2010 Fortbildungslehrgang mit Zertifizierungsprüfung „IT-Sicherheitsbeauftragte I", seit 2017 Fortbildungslehrgang mit Zertifizierungsprüfung „Datenschutzbeauftragte nach der EU-DSGVO.*

***Karin Wilhelm** arbeitet im Bundesamt für Sicherheit in der Informationstechnik (BSI) im Referat „Cyber-Sicherheit für Bürger und Gesellschaft". Im Rahmen der Awareness-Arbeit unterstützt sie Verbraucher und Verbraucherinnen dabei, sich sicher und selbstbestimmt durch die digitale Welt zu bewegen.*

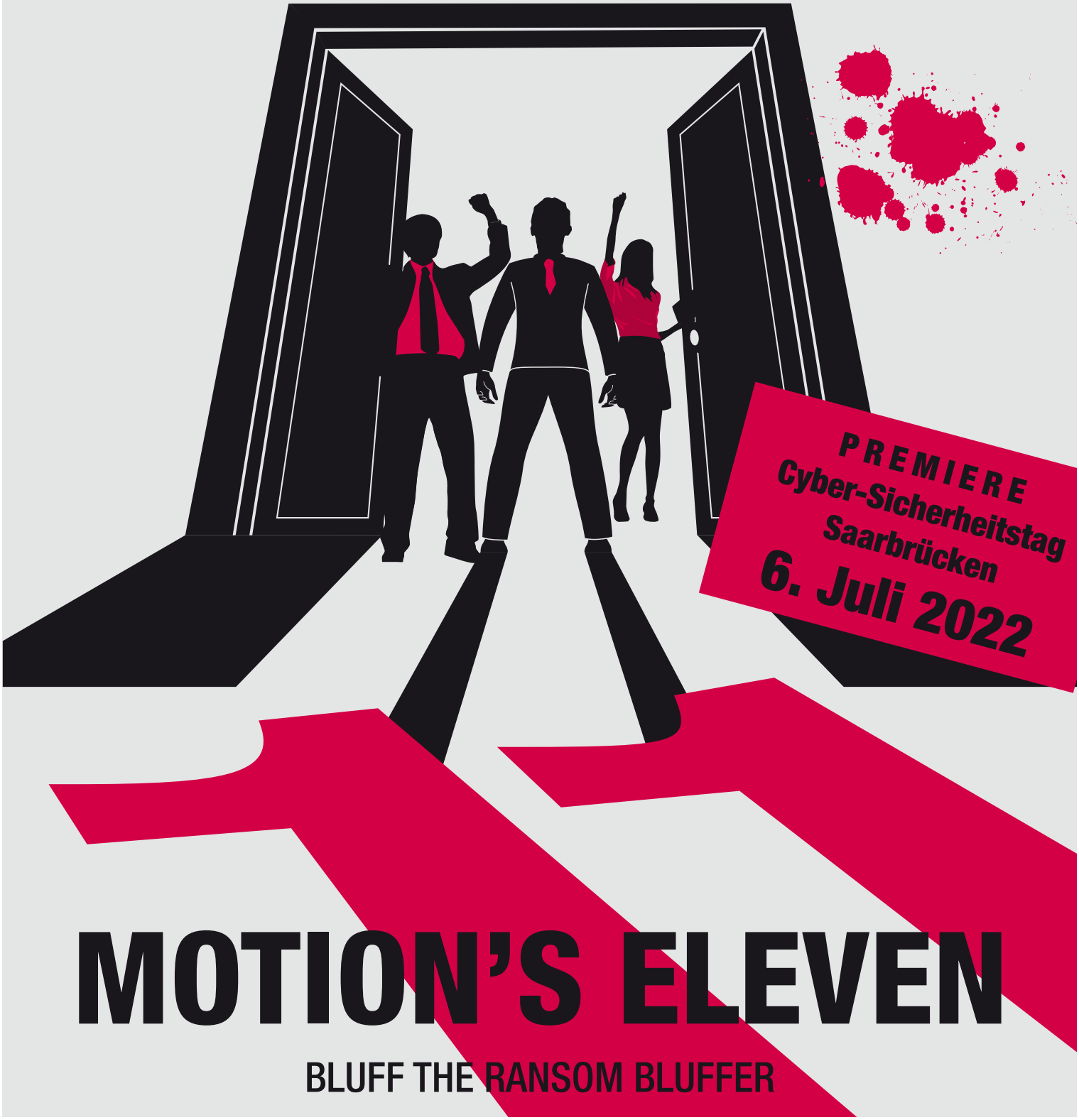
ADAM & EVA

Idee: Rainer Ariing

FEATURING KENNY MOTION & THE HACKING GANG | FRED BURNER | MAIGRITT SANDBERGER |DU SELBST SOWIE

RANSOM WARE | SPEAR PHISHING | MAL WARE | MELDE WEGE | BACK UP

CYBER SECURITY ESCAPE ROOM



K4 DIGITAL

known_sense
awareness you can touch.

Mittelstand 4.0
Kompetenzzentrum
Saarbrücken

saaris
saarland.innovation&standort e.V.