known_sense

awareness you can touch.

Security Awareness für Anfänger

known_sense-Intro-Bildstrecken-Erklärbuch

known_sense

awareness you can touch.

Warum Informationssicherheit zu paradoxen Verhältnissen führt?

Kennen Sie sich mit Psychologie aus? Selbst, wenn Sie kein Psychologe sind, vermutlich „so ein bisschen", etwa als Sofa-Laie – und ein bisschen „Supermarkt-Psychologe" muss ja heute sein, wenn man mitreden will.

In Bezug auf Security Awareness ist das besonders wichtig. Denn Sie werden uns zustimmen, dass heute kein Innovationsprojekt, kein Veränderungsmanagement ohne Berücksichtigung des Seelenhaushaltes der Menschen auskommt. Ohne Analyse der Lebensumstände oder Coaching läuft gar nichts. Nur welche Psychologie (?) ist hier die Frage. Es gibt ja mehr als ein paar Dutzend psychologischer Schulen.

Wir empfehlen bei der Arbeit mit Security-Kommunikation tiefenpsychologische, morphologische Verfahren, die den Erklärungen des menschlichen Verhaltens und Erlebens einen hohen Stellenwert beimessen. Vielleicht haben Sie schon einmal von dem Marktforschungsinstitut rheingold gehört? Die zentrale Idee der dort weiterentwickelten, tiefenpsychologischen Methode, die wir für das Thema Security nutzen, ist, dass „unter der Oberfläche" des Bewusstseins (etwa jenseits einer sog. Cover Story) in den „tieferen" Layern der Psyche weitere, unbewusste Prozesse ablaufen, die das bewusste Seelenleben (etwa die sog. Impact Story) stark beeinflussen.

Sie kennen vielleicht den Vergleich mit dem Eisberg, von dem der größte Teil nicht sichtbar ist. Das, was unter der Oberfläche schwimmt, wäre das Unbewusste und es hat einen höheren Anteil an unserer eigenen Wirklichkeit, als wir ggf. einräumen würden, weil wir uns selber nach Außen überwiegend sachlich-kontrolliert erleben. Das Paradoxe in der Sicherheit ist dominanter als in vielen anderen Lebensbereichen und wird geprägt von den kleinen, inneren Grabenkämpfen zwischen unserer sachlich-rationalen, kognitiven Verfassung und unserem Unbewussten.

known_sense

awareness you can touch.

Warum Menschen das Ent-Sichern leichter fällt als das Absichern.

Das Unbewusste schlägt uns manchmal ein Schnippchen, indem es – aus Sicht unserer Kognition – unerklärliche Dinge unternimmt, z.B. sich ent-sichert, obwohl wir es – etwa aus Compliancegründen (z. B. basierend auf Policys) – eigentlich besser wissen müssten.

D. h es gibt immer die zwei Seiten der Medaille. Die eine will sichern, die andere nicht. Da aber SICHERUNG stets auch etwas Passives beinhaltet – ein Abschließen kann ggf. auch als Einschließen wahrgenommen werden, denn in einer Burg ist man vielleicht sicher, bei Belagerung von außen aber auch wie in einem Sarg stillgestellt – giert die andere Seite in uns nach menschlichen Eröffnungen. D. h. Menschen sind mental in der Regel um Ausgleich dieser morphologischen Phänomene, eben der 2 Seiten einer Medaille, bemüht.

Auf diese Weise entstehen etwa auch viele sog. „unbeabsichtigte Fehler" in der Information Security, Fehler, die sich auf Sicherheit auswirken und die mit dem Paradoxen zusammenhängen. Man kann sogar sagen, dass Sicherheit ganz besonders paradox ist, weil wir wissen, dass sicheres Verhalten – das betrifft jetzt nicht nur die Infosec – eine Form der Still-Legung, im worst case bis zu Stillstand, also dem Tod, bedeutet. Wenn man die „Black Box Mensch" entschlüsseln will, um zu verstehen, welche Sinnhaftigkeit in sog. „Fehlern" stecken und wie man die Menschen in ihrer Ganzheit aus Verstand und Seele ansprechen muss, um erfolgreiche Awareness-Kampagnen zu gestalten, sollte man das Paradoxe und die tifenpsychologischen Methoden nutzen.

Nachlesen können Sie dies alles unter anderem in unserer allerersten tiefenpsychlogischen Security-Studie von 2006, „Entsicherung am Arbeitsplatz", in der wir „geheime" Motive für Fehlleistungen in der Informationssicherheit entschlüsselt haben.

known_sense

awareness you can touch.

Warum Lernen nicht ausreichend ist, um Menschen zu sensibilisieren.

Ausgehend von den genannten, psychologischen Phänomenen wird klar, dass es bei Awareness nicht damit getan ist, die Lerntheorie in einer Form umnzusetzen, dass man Mitarbeiter Wissenshäppchen über Lehrbücher und Schulfernsehen-Videos in deren Köpfe implementiert.

Und der Controler von Leonie, der nach einem CEO-Fraud 2016 Cyberkriminellen freiwillig 40 Mio. Euro überwiesen hat, war ja auch beileibe nicht eingeschränkt denkfähig, sondern vermutlich sogar ein sehr intelligenter Mensch.

Sicheres Verhalten hat also mit Intelligenz kaum etwas zu tun. Sicheres Verhalten ist vor allem Motivationssache. Fühle ich mich auf der Arbeit wohl? Brenne ich für das, was ich tue? Was habe ich persönlich davon, ggf. sorgsamer und langsamer zu arbeiten, um die Sicherheitsmaßnahmen einzuhalten – außer dass der Chef mich eventuell dafür tadelt, weil ich nicht fertig geworden bin? All das sind emotionsgeleitete Qualitäten, die mit Lernen nicht oder kaum adressiert werden können. Also müssen Awareness-Maßnahmen eben vor allem emotionale Faktoren – die Impact-Story unter der glatten Oberfläche unseres Verstands – bewegen.

known_sense

awareness you can touch.

Warum Bindung und Gemeinschaft der Kit für eine bessere Defense sind.

Wenn ich emotionale Maßnahmen in die Awarenesskampagne integriere, muss ich neben der auf Lerntheorie beruhenden Wissensvermittlung auch Marketing berücksichtigen. Aber auch Marketing ist eine Einbahnstraße, wenn ich das, was ich ggf. über einen Kanal ohne Rückkanal sende, nicht in Kopf und Bauch meiner Zielgruppe verankern kann.

Also fehlen dem klassischen Schulfernsehen und dem reinen Promoten weitere Elemente, die die Nachhaltigkeit von Awareness-Botschaften sichern.

Es ist in diesem Kontext vor allem der Bezug zur sog. systemischen Kommunikation, der die Königsdisziplin von Awareness darstellt. Die systemische Kommunikation schaut auf den Kontakt zu sich selbst und innerhalb einer Organisation auf den zu den mich umgebenden Menschen und hat mehr mit Selbstreflektion und Beziehung zu tun als mit einer klassischen Lern- bzw. Werbestrategie.

known_sense

awareness you can touch.

Warum das Sprechen über Sicherheit der Schlüssel zu mehr Nachhaltigkeit ist.

Wenn systemische Kommunikation und die Gemeinschaft die Schlüssel für Nachhaltigkeit in der Awareness sind, muss ich nochmals zurückschauen auf das Lernen und das Marketing und mich fragen, welche Ideen bzw. Elemente Bindung und Gemeinschaft fördern.

Man gelangt in der Rückschau relativ bald zur diskursiven bzw. konstruktivistischen Didaktik. Lernen ist nämlich nicht immer gleich Lernen – es kommt am Ende darauf an, WIE das Wissen vermittelt uns rezipiert bzw. „verarbeitet" wird.

Die konstruktivistische Didaktik fördert das Lernen als Prozess, die diskursive das Lernen im Austausch – wir nennen dieses Prinzip „Talking Security" – also das Sprechen über Sicherheit verankert einen Lernprozess stärker als andere, klassische didaktische Ansätze, weil der Kontakt auf Augenhöhe zu anderen, z. B. innerhalb eines Teams, uns berührt und wir uns mit diesen Kollegen und Kolleginnen vergleichen können. „Wer bei uns nutzt Schatten-IT als Bypass – mit welchen Folgen für die Security? Und warum ist das so?" Usw.

Darüber, über Fehlerkultur und die Sicherheitsmaßnahmen, die ggf. compliant sind, aber das Arbeiten verkomplizieren – z. B. das Arbeiten im Home Office – muss so offen und so kontrovers wie möglich gesprochen werden. Erst durch diesen Austausch wird gewahr, wie wichtig ggf. Details in der Infosec sind. Somit kann ich Inhalte von Kampagnen auch besser memorieren – eben weil diese mit positiven, berührenden Erlebnissen belegt sind.

known_sense

awareness you can touch.

Warum Spielen das neue Lernen ist.

Haben Sie schon einmal an Plan- oder Unternehmensspielen teilgenommen? Wenn nicht, haben Sie etwas verpasst.

Denn durch das Kommunizieren beim Spielen erhalten Team-Formate – vor allem hinsichtlich der Change-Idee – einen ganz eigenen, höheren Stellenwert als z. B. das einsame Erledigen von Trainings vor dem Bildschirm via WBTs & Co.

Und gerade Team-Formate funktionieren am besten vor dem Hintergrund regelbasierter Settings – und das sind nun mal Spiele.

Der Benefit von Gamification in Organisationen besteht darin, Systeme, Prozesse, Komplexität ohne bzw. mit nur geringer Reaktanz einzuführen, umzuwandeln oder zu betreiben. Damit dienen Security-Games der Wissens- bzw. Erfahrungsvermittlung, der Emotionalisierung, der Interaktion, zur Motivation, als Problemlöser oder Involvierer, um erwünschte Verhaltensweisen annehmen zu lassen (empathiebasierter, diskursiver Ansatz) – zusammenfassend um eine Wertschöpfung für alle Beteiligten zu erreichen.

Denken Sie dabei stets an den Menschen als sog. „Homo Ludens", der ohne Ausprobieren, ohne Spiel nicht zu einer Entwicklungsleistung fähig ist. Und durch das Regelbasierte ist Spielen eh eine Ähnlichkeit zur Infosec inhärent, die ja auch möglichst regelbasiert funktionieren soll.

known_sense

awareness you can touch.

Warum sexy Security die Motivation zu sicherem Verhalten steigert.

Lernen, Emotionalisierung bzw. Diskurse mithilfe von Spielen werden grundsätzlich von den meisten Mitarbeitenden attraktiver als E-Learnings, Powerpointschlachten in Classroom-Settings oder Erklärfilmchen eingeschätzt.

Vor allem der Kontakt zu Kollegen und Kolleginnen wird wertgeschätzt. Ausschließliche Nutzung von Gamification macht aber aus einer Kampagne noch lange keinen Mega-Erfolg. Erfolgreich sind Kampagnen dann, wenn sie auf Basis integrierter Kommunikation im wohltemperierten, schlauen Mix aus sämtlichen verfügbaren Medien und Kanälen angeboten werden, d. h. analog und digital, ausführliche Inhalte und kurze Clips, alleine und gemeinsam – eben für jeden Lerntypen ein Portfolio aus passenden Lern-, Marketing und systemischen Empowerment-Tools.

known_sense

awareness you can touch.

Warum emotionale Führung jeden Außenkontakt zu Social Engineers überflüssig macht.

Sind Sie jemals von einem Social Engineer angegriffen worden? Wenn Sie jetzt mit „Nein" antworten, war Ihnen das vermutlich gar nicht aufgefallen.

Erinnern Sie sich an die kurze Definition von systemischer Kommunikation? Die umfasst nämlich nicht nur den Kontakt zu anderen im Team – wie oben beschrieben – sondern auch den Kontakt zu sich selbst.

Wir behaupten, jemand, der sich nicht kennt, weil er nicht mit sich im Kontakt ist, ist aus Sicht der Informationssicherheit ein permanentes Risiko. Jetzt könnt man sagen: Irgendwo hört die Verantwortung von Informationssicherheit bzw. Organisation auf – man kann sich nicht um alles kümmern, was ggf. Kollateralschäden auslöst. Das ist soweit richtig. Bedenken Sie jedoch: Social Engineering (SE) ist seit einigen Jahren das Informationssicherheitsrisiko Nummer 1. Auch wenn die IT-Security die Technik und Prozesse immer besser in den Griff bekommt – bei SE ist der Mensch auf das Menschsein zurückgeworfen. Es gibt leider keinen Social Engineer-Scanner, der wie ein Virenscanner für Sauberkeit sorgt. Die Einschätzung, wem man vertraut und wem nicht, obliegt alleine dem Menschen und ist oftmals Bauchgefühl bzw. Intuition.

Die wichtige Frage jedoch im Zusammenhang mit der hiesigen Ausgangsbotschaft: Wie sollen Mitarbeitende Fremde, mithin die Motive von Social Engineers zu täuschen, beurteilen, wenn sie sich nicht selbst gut genug kennen? Wir stellen in unseren Studien immer wieder fest, dass dies ein großes Problem ist.

Eine Sensibilisierung zum Thema Social Engineering muss also auch die Selbstreflexion umfassen: Was sind meine kommunikativen Stärken, wo sind meine Schwächen, d.h. welches soziale Einfalltor – Druck, Anerkennung, Hilfsbereitschaft usw. – würde ein Täter adressieren, um bei mir an Informationen zu gelangen?

known_sense

awareness you can touch.

Warum Achtsamkeit bedeutsamer ist als Wissensvermittlung.

Gerade beim Thema Social Engineering kommt das Thema Achtsamkeit ins Spiel. Achtsamkeit ist stets Teil der intendierten Awareness. Mit ihr ist die mentale Fähigkeit gemeint, die auf das eigene Wirken gerichtete Aufmerksamkeit ohne Vergessen bzw. Ablenkung aufrechtzuerhalten.

Damit ist Achtsamkeit die Fähigkeit, die bemerkt, dass Ablenkung stattgefunden hat mit der Folge, dass Aufmerksamkeit wieder aktiv hergestellt werden kann. Dies lässt sich einüben. Es handelt sich also beim Megatrend Mindfulness bzw. bei MBSR (Mindfulness Based Stress Reaction) um pures Handwerk.

Die SAP AG hat MBSR-Maßnahmen zur Gesundheitsfürsorge bereits seit vielen Jahren in ihr Corporate Health Programm aufgenommen. Aktuell gibt es hierzu keine Studie, aber wir möchten jede Wette eingehen, dass ein derartiges oder vergleichbares Programm auch auf das Thema Sicherheit einzahlt.

known_sense

awareness you can touch.

Warum wir uns selber kennen lernen müssen, um die Motive Fremder beurteilen zu können.

Es gibt aber noch andere Faktoren, die produktiv auf das Risiko Social Engineering einzahlen. „Gute" Führung! Denn Führung ist ja per se soziale Einflussnahme auf Menschen – aus unserer Sicht die produktiver als der Einfluss von Cyberkriminellen. Aber man sollte diesen nicht unterschätzen.

Für Mitarbeitende, die etwa nicht vom Chef gelobt werden, ist ein Außenkontakt zu einem Hacker besser als gar keiner. Daher kann man sagen: „Ganz schön blöd, wenn der Social Engineer der netteste Mensch am Arbeitsplatz ist." Emotionale Führung, die u. a. auch Anerkennung verteilt, ist daher ein wichtiger Faktor für die soziale Temperatur am Arbeitsplatz und eine risikofreie Arbeitsumgebung. Daher gilt es, in Awareness-Kampagnen gerade auch Führungskräfte auf Ihre Sicherheitsrolle einzuschwören Manager sind Vorbilder und Multiplikatoren – und sie können Social Engineering verhindern.

known_sense

awareness you can touch.

Wer Menschen sensibilisieren will, muss sie berühren.

Für weitere Fragen

known_sense
Jakob-Engels-Str. 39
51143 Köln

Fon +49 2203 1831618
sense@known-sense.de
www.known-sense.de