Neue Narrative für Informationssicherheit

David Scribane

etomer GmbH / SECUTAIN
david.scribane@secutain.com

Zusammenfassung

Das Etablieren eines angemessenen Levels für Informationssicherheit ist für jede Organisation eine Voraussetzung, um handlungsfähig zu bleiben und zu überleben. Um dies zu gewährleisten, sind neben technischen und organisatorischen Maßnahmen die Mitglieder einer Organisation – also die Beschäftigten einer Firma – ein wichtiger Faktor für die Wahrung der Informationssicherheit. Somit gehört es auch dazu, dass der Mensch in das Zentrum der Informationssicherheit gestellt wird. Dies wird durch verschiedene kommunikative Maßnahmen erreicht. Damit diese erfolgreich und nachhaltig zu einer Sensibilisierung der Beschäftigten und zu einer nachhaltigen Steigerung der Awareness führen, sind verschiedene Aspekte zu betrachten, die im Folgenden erläutert werden.

1 Anlass und Problemstellung

Das Bewusstsein für Informationssicherheit ist in den letzten Jahren in breiten Bevölkerungsschichten gestiegen. Dies liegt vor allem an der Nachrichtenlage, in der entsprechende Themen stärkere Betonung finden. Seien es die Enthüllungen von Edward Snowden, die Bedrohung kritischer Infrastrukturen durch Trojaner und Viren oder die Einflussnahme auf das Verhalten von Wählern durch soziale Netzwerke. Trotz der prominenteren Betonung dieser Themen, ist die Verunsicherung und das unbestimmte Gefühl, diesen Bedrohungen nicht gewachsen zu sein, bei einem Großteil der Bevölkerung und der Arbeitnehmer stark ausgeprägt. So sind nur 36% aller IT-Nutzer davon überzeugt, sich und ihre Informationen effektiv schützen zu können [Schul17].

Um dieser Verunsicherung entgegenzuwirken, verfolgen Organisationen zwei parallele Strategien: die Errichtung von organisatorischen und technischen Maßnahmen sowie die Sensibilisierung von Beschäftigten.

1.1 Organisatorische und technische Maßnahmen

Organisationen etablieren organisatorische und technische Maßnahmen zum Schutz von Informationen und IT-Systemen. Diese Maßnahmen werden in der Regel unter einem Informationssicherheitsmanagement-System (ISMS) gebündelt. In Deutschland finden dabei vorrangig die Systeme ISO 27001 und BSI IT-Grundschutz Anwendung.

Das Etablieren entsprechender Managementsysteme bedeutet einerseits einen erheblichen Aufwand finanzieller Mittel, um technische Maßnahmen zu etablieren, aktuell zu halten, zu warten und zu überwachen, um als Organisation gegen Angriffe wehrhaft zu bleiben und im Wettrüsten mit den existierenden Bedrohungen nicht ins Hintertreffen zu geraten. So gaben Anfang des

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 26-34.

Jahres 78% der deutschen Unternehmen an mehr oder deutlich mehr in IT-Sicherheit zu investieren [Bitk18]. Die eingesetzten Mittel sind dabei Virenscanner, Verschlüsselung, mehrstufige Firewalls, Big Data-Technologien für das Trennen von ungewünschten Angriffen und gewollter Kommunikation etc.

Auf der anderen Seite bedeutet das auch, dass aus Sicht des Mitarbeiters Regelwerke und Policies in diesen Bereichen qualitativ und quantitativ zunehmen. Dies wird insbesondere dadurch katalysiert, dass sich sowohl gesetzliche und regulatorische Vorgaben verschärfen (IT-Sicherheitsgesetz, EU-Datenschutzgrundverordnung) als auch Informationssicherheitsmanagement-Systeme (ISMS) eine stärkere Verbreitung finden.

1.2 Sensibilisierung von Beschäftigten

Von den Beschäftigten wird von den Führungsebenen von Organisationen erwartet, dass die zuvor genannten organisationalen Regeln und Policies wahrgenommen, verstanden und gelebt werden. Um dies zu unterstützen, werden kommunikative und qualifizierende Maßnahmen aufgesetzt, die zum Ziel haben sollen, ein höheres Maß an Awareness in einer Organisation zu erreichen.

Der Erfolg dieser Kommunikations- und Qualifizierungsmaßnahmen bemisst sich nicht nur in der Erfüllung sämtlicher Sensibilisierungs- und Schulungsvorgaben der anzuwendenden Rahmenwerke (EU-Datenschutzgrundverordnung, IT-Sicherheitsgesetz, ISO 27001, BSI IT-Grundschutz etc.), sondern in der tatsächlichen, gelebten höheren Sensibilität einer Organisation für das Thema Informationssicherheit.

Dass dies eine große Herausforderung darstellt, zeigt sich darin, dass 82% der IT-Verantwortlichen in Organisationen beklagen, dass Regeln zum Thema Informationssicherheit nicht bekannt sind [Pone17]. 21% der Beschäftigten fällt es nach eigener Aussage „schwer, mit den sich ständig ändernden IT-Sicherheitsrichtlinien Schritt zu halten“. [Dell18]

Doch nicht nur Richtlinien, sondern auch die technische Entwicklung führt zu Herausforderungen. Anwender sehen sich einer permanent komplexer werdenden Technik und einer immer höheren Informationsdichte gegenüber. Dies führt zu Unsicherheit und ungewolltem Verhalten, das die Sicherheit der Informationen gefährdet. Im schlimmsten Fall werden so Anwender unwissentlich zum Sicherheitsrisiko, da immer kreativere Angreifer mit immer ausgeklügelteren Methoden versuchen, diese Unbedarftheit und Unsicherheit auszunutzen, um Informationen zu stehlen, zu verändern oder IT-Systeme zu kompromittieren.

Ziel muss es sein, Anwender so zu befähigen und zu stärken, dass sie vom Sicherheitsrisiko zum Teil der Sicherheitskette werden. Die Achtsamkeit jedes Einzelnen führt im Ergebnis zu einer achtsamen Organisation, die viel besser gegen Angriffe geschützt ist und im Falle eines Vorfalls rechtzeitiger und besonnener reagieren kann.

Die Erfahrungen der letzten Jahre zeigen, dass dies ein beschwerlicher Prozess sein kann, da

- Erfolge nicht kurzfristig eintreten, sondern eher einen Kulturwandel hervorrufen oder begleiten können und damit eher langfristig zu erwarten sind,
- Erfolge stark abhängig von der Fehler- und Unternehmenskultur sind,
- das Thema Informationssicherheit aufgrund seiner Komplexität und seiner Abstraktheit von Anwendern gerne mit spitzen Fingern angefasst wird,

- der Bezug zur eigenen Lebenswirklichkeit bei der Vermittlung von Themen rund um die Informationssicherheit nicht immer gegeben ist,
- bestehende Policies als zu wenig zugänglich oder übertrieben restriktiv wahrgenommen werden und
- Policies in ihrer Charakteristik als nicht hinreichend wahrgenommen werden, da sie eine erfahrungsbasierte Perspektive einnehmen und keine Aussagen oder Handlungshinweise für zukünftige, heute noch unbekannte Bedrohungslagen liefern.

2 Kommunikative Grundsätze

Aus der angeführten Erkenntnis ergeben sich fünf wichtige Punkte, die für eine erfolgreiche und nachhaltige Kommunikation für die Awarenessbildung in Organisationen notwendig sind.

2.1 Ambidextrie

Das nachhaltige Bewahren eines hohen Niveaus von Informationssicherheit ist ein fortwährender Prozess, da mit dem stetigen technischen Wandel die Veränderung von Risikolagen einhergeht. Das Verhalten von Mitgliedern einer Organisation muss daraufhin angepasst werden, was sich in angepassten oder neu etablierten Sicherheitspolicies niederschlägt. Darüber hinaus muss davon ausgegangen werden, dass die Organisation Bedrohungen ausgesetzt sein wird, die heute noch unbekannt sind, weshalb für diese Situationen noch keine Regulatorik geschaffen werden konnte.

Für eine dauerhaft wehrhafte Organisation ist eine organisationale Ambidextrie (Beidhändigkeit) notwendig, die sich durch die gleichzeitige Ausprägung von Exploitation und Exploration auszeichnet [TuRe13]. Dieses Konzept verfolgt heruntergebrochen auf das Thema Informationssicherheit sowohl die Herstellung einer Resilienz (Wehrhaftigkeit) gegen aktuelle Bedrohungen, für die Regel entwickelt und kommuniziert worden sind als auch gegen zukünftige, heute noch unbekannte Bedrohungen, für die heute und auch zum Zeitpunkt des Eintretens noch kein Regelwerk existiert.

Exploitation beschriebt dabei das Konzept des Erreichens einer proaktiven Robustheit einer Organisation. Durch die Internalisierung von bestehenden Regeln, die Sicherheitsrichtlinien oder Beschäftigtenpolicies, werden die einzelnen Mitglieder einer Organisation in die Lage versetzt, in vorhersehbaren Situationen eine von ihnen erwartete Reaktion zu zeigen. Dies kann dadurch erreicht werden, dass kommunikative Maßnahmen in leicht verständlicher, angebracht portionierter Weise, mit unterschiedlichen Schwerpunkten versehen über einen längeren Zeitraum kommuniziert werden. Dies können Unterweisungen, Schulungen, Lehrmaterialien etc. sein. Die konkrete Ausprägung der Kommunikationsmaßnahmen ist dabei von unterschiedlichen Rahmenbedingungen, wie erwartete Ansprache der Mitarbeiter, Altersstruktur, örtliche Verteilung, zur Verfügung stehende Medien etc., abhängig.

Die Exploration befasst sich im Gegensatz zur Exploitation mit unvorhersehbaren Situationen, von denen die Thematik Informationssicherheit aufgrund des stetigen Wandels permanent betroffen ist. Mit ihr soll eine reaktive Agilität der Organisation erreicht werden. Dies bedeutet, dass in Situationen, die heute nicht vorhersehbar sind und für die heute noch kein Regelwerk existiert, dennoch im Sinne der Regeln gehandelt wird [KoEh14].

Dies setzt voraus, dass die Organisation die Regeln nicht als kontextloses, stur zu befolgendes Regelwerk wahrnimmt, sondern den Sinn der Regeln verstanden hat und deren Ziel verfolgt –

selbst wenn das Erlebte von den darin beschriebenen Situationen abweicht. Dies kann erreicht werden, indem das Thema Informationssicherheit entsprechende Handlungsspielräume dem einzelnen Individuum lässt und Verantwortliche für dieses Thema die Neugier für das Thema fördern und eine kommunikative Basis erstellen, in der Kommunikation auf Augenhöhe stattfinden kann.

2.2 Aufbau von Sympathie und Wissen

Um eine nachhaltige Verhaltensänderung bei den Mitgliedern einer Organisation zu bewirken, ist es notwendig, dass zwei Ebenen bedient werden:

- Die kognitive Ebene – sie beschreibt das Wissen um die Sache also im Bereich Informationssicherheit die Kenntnis über potenzielle Gefahren, die Relevanz der Informationssicherheit und entsprechende Richtlinien im Unternehmen.
- Die emotionale Ebene: Sie beschreibt, wie viel Sympathie (Sicherheit als positiv assoziiertes Gefühl) oder Antipathie (Sicherheit assoziiert als lästige Vorschriften, die den persönlichen Handlungsspielraum einschränken) eine Person einer Thematik entgegenbringt.

Die Wissensvermittlung erfolgt umso besser, je greifbarer und anschlussfähiger ein Thema kommuniziert wird. [Rück14] Das bedeutet, dass der individuelle Erfahrungshintergrund einer Person mitbedacht werden muss, damit das Thema verständlich kommuniziert wird. Dies kann durch Analogien geschehen; dies können auch gemeinsame Erfahrungen der Zielgruppe sein, auf die sich bezogen wird. Je konkreter die Handlungsempfehlungen sind, desto besser können sie umgesetzt werden.

Ein Beispiel für verständliche Analogien: Wenn wir uns ins Auto setzen, schnallen wir uns automatisch an. Wir denken gar nicht mehr darüber nach. Selbst bei kurzen Strecken. Die Kassiererin im Supermarkt schließt nach jedem Bezahlvorgang die Kasse, obwohl der nächste Kunde schon wartet und sie in 2 Minuten wieder in die Kasse greifen muss. Aber das ist eine Sicherheitsmaßnahme, die mittlerweile automatisch durchgeführt wird. Wenn wir mit dem Auto unterwegs sind, halten wir an der roten Ampel an – auch wenn es nachts ist und kein weiteres Auto weithin sichtbar ist. Nur wenn wir kurz den Arbeitsplatz verlassen, sperren wir nicht den Rechner und geben anderen Zugriff auf unsere Daten und die Information unserer Organisation?

Die Kommunikation sollte so gestaltet sein, dass der Empfänger sich die Fragen beantworten kann: Was hat das mit mir zu tun? Was bedeutet das für meinen Arbeitsplatz? Was bedeutet das für mein Privatleben? Häufig ist das Privatleben eine große Motivation, sich mit der Thematik zu beschäftigen. Verantwortliche für das Thema Informationssicherheit sollten demnach auch für private Fragestellungen zur Verfügung stehen und auch kommunikative Elemente, die diesen Bereich flankieren, nicht scheuen, da dadurch sowohl die kognitive als auch die emotionale Ebene bedient werden. Das für den privaten Bereich erworbene Wissen wird durch die Beschäftigten auch im beruflichen Kontext wiederverwendet und führt so zu einer Steigerung der Awareness für Informationssicherheit.

Ein häufig genutztes Beispiel hierfür ist das Thema Instant Messaging. Treten Beschäftigte an den IT-Sicherheitsbeauftragten heran und möchten wissen, wer auf die versendeten und empfangenen Nachrichten, die zum Teil sehr private und intime Informationen enthalten, auf ihrem privaten Smartphone zugreifen kann, kann dies als Anlass genommen werden, um das Prinzip

der Ende-zu-Ende-Verschlüsselung oder der Schlüsselhoheit zu erklären. Informationssicherheit wird so ganz unterschwellig zum Pull-Request anstatt, dass entsprechende Themen in die Organisation getragen werden müssen.

Humor und unterhaltende Elemente wecken darüber hinaus Sympathie für die Thematik. Der Moderator der US-amerikanischen Comedy-Nachrichten-Sendung „Last Week Tonight“ John Oliver, der zur besten Sendezeit einen 25-minütigen Beitrag über Kryptowährungen präsentiert hat, erläuterte, dass er das Thema so aufbereitet hat, wie er es seinem Ich von vor drei Wochen erklären würde, als er noch keine Ahnung von dem Thema hatte. Das vermeintlich trockene Thema Informationssicherheit kann darüber hinaus durch unterhaltsames Storytelling, die Nutzung persönlicher Medien, wie Blogs, persönliche Newsletter des Sicherheitsbeauftragten, Podcasts etc. aufgewertet werden. Diese Medien ermöglichen eine informellere Tonalität, meinungsstärkere Äußerungen und bieten teilweise einen Rückkanal für Rückmeldungen aus der Belegschaft.

Dies trägt auch zu einer Kommunikation auf Augenhöhe bei, die wichtig für die Sympathie für das Thema ist und somit ein wichtiger Baustein für die nachhaltige Handlungsänderung von Beschäftigten. Kommunikation zum Thema Informationssicherheit sollte so gestaltet sein, dass sie nicht als Bevormundung, Komforteinschränkung und lästige, unverständliche Regulatorik angesehen wird, sondern vielmehr als Hilfestellung zur Förderung der Informationssicherheit, die relevant ist für das Überleben und die Leistungsfähigkeit der Organisation. Bestenfalls verstehen sich Beschäftigte durch die geschickte Kommunikation als Teil einer Allianz des Guten, die gemeinsam gegen die Gefahren und Angriffe sich zur Wehr setzen und das gemeinsame Ziel des Schutzes der Organisation verfolgen.

2.3 Überwinden der Fachsprache

Gerade die Informationssicherheit ist gespickt mit Fachbegriffen und Akronymen, die die Zugänglichkeit zu der Thematik erheblich erschweren. Ist unter Experten die Anwendung von Fachsprache wichtig und sinnvoll,

- da so effizient kommuniziert werden kann, weil
- dahinterliegende Konzepte nicht erläutert werden müssen und
- Missverstände vermieden werden etc.,

so ist diese Fachsprache in der awarenessbildenden Kommunikation insbesondere in Richtung wenig technikaffiner Personen möglichst zu vermeiden. Darüber hinaus besitzt Fachsprache die Wirkung der Kodierung, die eine Unverständlichkeit des Gesagten für Dritte zum Ziel hat. Außerdem kann mit der Anwendung von Fachsprache die Legitimierung des Expertenstatus‘ eines Redners erfolgen. Diese beiden Effekte sind jedoch im Rahmen von Awarenesskommunikation ungewünscht, da sie sprachliche Barrieren zwischen dem Sender und dem Empfänger einer Botschaft aufbauen. Sollte es nicht möglich sein, Fachsprache zu vermeiden, so sind Konzepte hinter den Begriffen so zu erklären, dass das Prinzip möglichst leicht verstanden wird. Dabei helfen Analogien sowie Beschreibungen der konkreten Auswirkung auf den beruflichen und privaten Kontext des Empfängers der Kommunikation. „Wenn das Bewusstsein für Security-Belange geschärft werden soll, muss die Fachsprachlichkeit aufgebrochen werden.“ [HeKl18]

So beschreiben Hessler und Klipper den kommunikativen Erfolg mit der Formel:

Gruppenerwartung * sprachliches Register = kommunikativer Erfolg

Dies legt dar, dass sowohl die Erwartungshaltung der Kommunikationsempfänger, deren Vorwissen und deren Aufgeschlossenheit zu dem Thema beachtet und in der Planung der Kommunikation berücksichtigt werden muss. Andererseits sind die richtigen sprachlichen Register zu ziehen. Dies umfasst das verwendete Vokabular und die genutzte Tonalität. Wird nur einem der Faktoren nicht die notwendige Aufmerksamkeit zu Teil oder falsch entschieden getroffen, so ist der Erfolg der Kommunikation gefährdet.

Abb. 1: Heartbleed-Logo

Einige Beispiele, wie die Kommunikation rund um den Heartbleed-Fehler, zeigen, wie erfolgreich entsprechende Maßnahmen sein können, wenn sie die Problematik verständlich illustrieren oder über die Kanäle kommunizieren, die der Benutzer erwartet (z.B. eigene Webseite für die Schwachstelle, Social-Media-Kanäle, Medienpartner etc.). Darüber hinaus zeigt dieses Beispiel, wie die vereinfachte Darstellung des der Sicherheitslücke zu Grunde liegenden Prinzips helfen kann, Verständnis für das Risiko zu wecken – ohne dabei für die breite Bevölkerung zu technisch zu werden (siehe Formel für kommunikativen Erfolg). Ein Beispiel dafür, dass trotz aller kommunikativen Zugänglichkeit und vereinfachten Darstellung von Sicherheitsproblemen mit dieser Methode verantwortungsvoll umgegangen werden muss, ist die Sicherheitslücke „E-Fail“, die im Mai 2018 veröffentlicht wurde. Diese beschreibt Lücken in diversen E-Mail-Clients, mit der das Mitlesen von sogar verschlüsselten E-Mails möglich wurde. Die verkürzte Darstellung in vielen Medien lautete: „Forscher knacken E-Mail-Verschlüsselung“, was fachlich falsch und in seiner Auswirkung weit zu dramatisch dargestellt wurde. [tage18]

2.4 Den Unterschied zwischen Schuld und Scham kennen

Verhält sich eine Person falsch, wie im Beispiel einer Phishing-Mail fühlt sie sich schuldig, da sie – als individuell wahrgenommen einzige Person – auf den Angriff hereingefallen ist. Vielleicht schämt sie sich sogar durch ihr unbedachtes Handeln, das im Nachgang durch sie häufig sogar als vermeidbar wahrgenommen wird: „Warum habe ich mich nur so dumm angestellt!?“

Viel intensiver werden die Gefühle der Schuld und Scham nach einer erfolgreichen Social Engineering-Attacke, bei der ein Angreifer – vielleicht sogar vorbei an allen technischen Schutzmaßnahmen – eine Zielperson psychologisch manipuliert, so dass sie Handlungen begeht, die sie unter anderen Umständen nicht begehen würde. Weil die Zielperson einer anderen Person – dem Angreifer – ihr Vertrauen geschenkt hat, wurde sie ausgenutzt. Da Social Engineering-Attacken menschliche Eigenschaften ausnutzen, also die Eigenschaften, die eine individuelle Person ausmachen, so wird die Ausnutzung dieser Eigenschaften als besonders verletzend empfunden. Zudem gibt es in diesem Falle sogar einen Zeugen der fehlerhaften Handlung: den Angreifer. Diese Gemengelage kann bei dem Opfer mehrere Reaktionen hervorrufen:

1. Soziale Isolation. Da die Verletzung beim Opfer so tief sitzen kann, kann es sein, dass aufgrund der empfundenen Scham das Opfer den sozialen Rückzug sucht, andere beschuldigt, die Situation beschönigt, Dinge verheimlicht oder in aggressiv wird.
2. Das Gefühl der Mittäterschaft. Da der Angriff nur aufgrund des Mitwirkens des Opfers erfolgreich verlief, kann es sein, dass das Opfer sich in der unfreiwilligen Täterrolle fühlt.

Ein erfolgreicher Angriff – und somit das eigene Scheitern des Opfers – schnell an die entsprechenden Stellen in der Organisation zu kommunizieren, fällt schwer, da der begangene Fehler Angst vor arbeitsrechtlichen Konsequenzen oder gesellschaftlicher Ausgrenzung hervorrufen kann. Scham löst häufig einen situativen sozialen Rückzug aus, was in dieser Situation genau das Gegenteil dessen ist, was erforderlich wäre. Das aktive und zügige Kommunizieren an die entsprechenden Stellen, damit die Organisation daraus lernen kann und wehrhafter wird, wäre der richtige Weg. [HaPo18]

Damit dieser Weg beschritten wird, ist es wichtig, in den awarenessbildenden Maßnahmen zu betonen, dass die Meldung solcher Vorfälle nicht geahndet wird, dies auch durch das Management bekräftigt wird und ggf. Personen zu benennen, die das Vertrauen der Beschäftigten genießen, denen sich anvertraut werden kann.

Das offene Aufbereiten einer erfolgreichen Attacke, was die Voraussetzung für eine lernende Organisation ist, darf somit niemals das Opfer bloßstellen – ggf. muss sie anonymisiert werden und muss jederzeit gesichtswahrend erfolgen. Das Opfer sowie die Arbeitnehmervertretungen sind dabei stets mit einzubeziehen und deren Anforderungen möglichst berücksichtigt werden. Das Opfer darf daher nicht als Täter, sondern vielmehr als wichtigen Zeugen einer alarmierenden Situation dargestellt werden. Die Aufbereitung der konkreten Vorfälle sollte derart gestaltet sein, dass der Empfänger der Kommunikation sich die Frage stellt: „Wäre mir das auch passiert?“ und „Wie hätte ich reagiert?“

2.5 Awareness für Informationssicherheit als Kulturwandel

Awareness für Informationssicherheit setzt eine offensive Fehlerkultur in einer Organisation voraus, denn trotz aller technischen und organisatorischen Maßnahmen sind häufig Menschen die letzte oder manchmal sogar die einzige Hürde, die Angreifer überwinden müssen. So funktionieren einige Angriffe nur, wenn der Benutzer aktiv unwissentlich den Angriff unterstützt. Dies ist beispielsweise bei einer Mailattacke der Fall, an denen Office-Dokumente hängen, die den Nutzer durch perfide Tricks dazu bewegen, die Makrofunktionen zu aktivieren, so dass Schadcode ausgeführt werden kann. Die Argumentationen der Angreifer, warum der Mitarbeiter diese möglicherweise sogar untersagte Handlung ausführen soll, können jedoch sehr überzeugend sein und insbesondere beim Spear-Phishing – also einer direkt auf das Opfer zugeschnittenen Attacke – so gestaltet sein, dass das Opfer bedenkenlos handelt. Der daraufhin erfolgreiche Angriff, der Daten- oder Identitätsdiebstahl, die Verschlüsselung wichtiger Informationen etc. zur Folge hat, entsteht demnach erst durch eine unachtsame Handlung eines Mitarbeiters.

Daher ist es wichtig, Beschäftigten die Sicherheit zu geben, dass das Melden dieses Angriffes unbedingt notwendig ist, um schnell und gezielt Gegenmaßnahmen zu ergreifen und diese Meldung keine oder nur marginale arbeitsrechtliche Maßnahmen nach sich ziehen wird. Awareness bedeutet auch, in einer lernenden Organisation zu agieren, die auch aus ihren Fehlern lernt. Häufig vertuschen Beschäftigte ihren eigenen Fehler, wenn keine ausgeprägte Fehlerkultur in

der Organisation existiert, wodurch die Situation entweder zu spät erkannt wird, durch den Angreifer wiederholbar wird oder in ihrer Auswirkung viel größer und gefährlicher werden könnte.

Ein Kulturwandel ist kein Prozess, der schnelle Ergebnisse erwarten kann. Vielmehr setzt sich eine Kultur für Informationssicherheit auch erst sukzessive in Organisationen durch. Aus diesem Grunde müssen Kampagnen für Informationssicherheit längerfristig angelegt werden, nicht den Eindruck eines Buschfeuers schüren und dauerhafte kommunikative Maßnahmen etablieren oder den Fokus auf diese lenken, falls diese bereits bestehen. Es muss dargestellt werden, dass Informationssicherheit kein Projekt, sondern ein dauernder Prozess ist.

Insbesondere in Organisationen, die bislang keine ausgeprägte Kultur oder Awareness für Informationssicherheit besitzen, kann es durch die Verantwortlichen für awarenessbildende Maßnahmen als frustrierend empfunden werden, wenn das Feedback sehr gering ist, dem Thema wenig Sympathie entgegengebracht wird oder sogar als lästig empfunden wird. In diesen Fällen sind das Durchhalten und das damit verbundene Signal, dass es sich hierbei um eine wichtige Angelegenheit handelt, erfolgsentscheidend.

Es existiert darüber hinaus keine allgemeingültige Messeinheit für die Bewertung einer organisationalen Awareness für Informationssicherheit. Dieser Umstand darf jedoch nicht dazu führen, dass awarenessbildende Maßnahmen nicht gemessen werden, wie es häufiger der Fall ist. So geben 40% der Unternehmen an, dass der Erfolg von Awarenessmaßnahmen nicht gemessen wird [Alli16]. Das Setzen von messbaren Zielen ist jedoch ein wichtiger Faktor für die Akzeptanz von awarenessbildenden Maßnahmen bei den unterschiedlichen Stakeholdern von awarenessbildenden Maßnahmen (Management, Compliance-Bereich, Personalvertretungen, IT, Anwender etc.). Die zu definierenden Ziele sind von Organisation zu Organisation sehr individuell und sind an den Zielen der der Maßnahmen auszurichten. Diese können eine schnellere oder vollständigere Rückmeldung von Sicherheitsereignissen sein genauso wie das Erreichen von weniger Sicherheitsereignissen im Umgang mit E-Mails oder eine höhere Sicherheit im Umgang mit gefährdeten Informationen oder IT-Equipment. Bei der Definition der Zielwerte ist darauf zu achten, dass sich Verhaltensänderungen erst sukzessive durchsetzen und vollständige Awareness nicht erreicht werden kann. Zudem sollte auf die Definition und die zu erwartenden Ziele achtgegeben werden.

Insbesondere im letzten Beispiel der skizzierten Zielstellungen kann es zunächst einen gegenteiligen Effekt geben: In einer Vorher-Nachher-Befragung sollen Mitarbeiter über einen Fragebogen zurückmelden, wie sicher sie sich im Umgang mit dem Internet und im Erkennen und Abwehren von Gefahren fühlen. Nach der Befragung werden awarenessbildende Maßnahmen durchgeführt, wodurch die Organisation eine höhere Sensibilität für dieses Thema erfährt. Im Anschluss wird die zweite Befragung mit der gleichen Fragestellung durchgeführt. Es ist zu erwarten, dass die Zahlen sich zunächst in die ungewünschte Richtung entwickeln – also die Beschäftigten melden zurück, dass sie sich unsicherer fühlen und sich bei Angriffen weniger gut zu verteidigen wissen. Dieser Effekt ist nicht selten, da die vorherige Sicherheit aus einer mangelnden Sensibilität für dieses Thema resultiert hatte. Die sensibilisierten Mitarbeiter verfügen jedoch nun nach der Durchführung der Awarenessmaßnahmen über ein anderes Wissen über die existierenden Gefahren und vertrauen somit bestimmten digitalen Kommunikationskanälen weniger als zuvor. Grundlage für diese Entwicklung ist jedoch eine höhere Awareness für das Thema, die es anzustreben gilt. Bei wirksamen dauerhaften Kommunikationsmaßnahmen sollte dieser Anfangseffekt jedoch negiert werden und dauerhaft eine höhere Sicherheit und Abwehrkompetenz entwickelt werden.

3 Resümee

Sensibilisierende Maßnahmen für das Thema Informationssicherheit können häufig ihre Wirkung verfehlen, wenn sie nicht optimal angelegt sind, die kommunikative Erwartungshaltung der Empfänger nicht berücksichtigen und die Wissensvermittlung den Hintergrund der Zielgruppen unberücksichtigt lässt. Daher ist bei der Planung und Durchführung von kommunikativen Maßnahmen

- sowohl auf die bestehenden Regeln hingewiesen werden als auch entsprechende Freiheiten in der Regelauslegung eingeräumt werden,
- mit der IT-Security Fachsprache gebrochen werden,
- keine kurzfristigen Erfolge erwartet werden, sondern eher ein nachhaltiges Ändern der Kultur unterstützen
- Strategien mit dem nicht sanktionierenden Umgang individueller Fehler berücksichtigen und
- darauf hinwirken, dass Sympathie und Wissen für das Thema Informationssicherheit aufgebaut werden, damit eine dauerhafte Verhaltensänderung bewirkt werden kann.

Literatur

[Schu17] H. Schuster: Gelangweilte Mitarbeiter sind größtes IT-Sicherheitsriko. In: https:// www. security-insider. de/ gelangweilte- mitarbeiter- sind- groesstes- it-sicherheitsrisiko-a-618881/ (2017).

[Bitk18] Bitkom Research: Live Security Studie 2017/2018. Bitkom research (2018) 5.

[Pone17] Ponemon Insititute: The Need for a New IT Security Architecture: Global Study (2017) 5.

[Dell18] DELL End-User Security Survey (2017) 8.

[TuRe13] C. A. O'Reilly III, M. L. Tushman: Organizational ambidexterity: Past, present, future.. In: Academy of Management Perspectives, 2013, Seiten 324-338.

[KoEh14] A. Kozica, I. Ehnert: Lernen von Nachhaltigkeit: Exploration und Exploitation als Lernmodi einer vollständig ambidextren Organisation (2014).

[Rück14] J. Rückert-John: Lernen durch Scheitern. Potenziale riskanter Veränderungsprozesse (2014).

[Oliv18] J. Oliver: John Oliver on His Children's Book About VP Pence's Gay Bunny, Marlon Bundo, https://www.youtube.com/watch?v=M5mFxEFxWrM (2018).

[tage18] tagesschau: Forscher knacken E-Mail-Verschlüsselung, https:// www. tagesschau. de/inland/e-mail-verschluesselung-101.html (2018).

[HeKl18] S. Hessler, S. Klipper: Warum finden Security-Experten so schlecht Gehör? – Sprachwissenschaftliche Konzepte zur Steigerung der Transmedialität des Sprachgebrauchs in der IT-Security, in: Sexy Security (2018).

[HaPo18] A. Haucke, D. Pokoyski: Mea culpa – Schuld, Scham und Opferrolle bei Social Engineering, <kes> – Die Zeitschrift für Informations-Sicherheit (2018) 6-7.

[Alli16] Allianz für Cybersicherheit, Bundesamt für die Sicherheit in der Informationstechnik: Ergebnisse der Awareness-Umfrage 2015 (2016) 27.