

Sie sind Informationssicherheitsbeauftragte(r) und haben daher die Aufgabe, Ihre Kolleginnen und Kollegen, deren primäres Ziel nicht Informationssicherheit ist, für das Thema zu sensibilisieren? Dann haben wir in diesem Beitrag einige Tipps und Empfehlungen – aus der Praxis und der Wissenschaft - zur Planung und Ausgestaltung Ihrer Security Awareness Maßnahmen.

EMPFEHLUNG 1: ZIEL FESTLEGEN

Es existieren verschiedene Security Awareness Definitionen wie z. B.:

- Bewusstsein für Angriffe schaffen;
- Bewusstsein schaffen, dass jeder mithelfen muss, damit ein angemessenes Schutzniveau für die eigene Organisation erreicht werden kann;
- Wissen vermitteln, wie Angreifer vorgehen bzw. wie man sich schützen kann,
- Wissen vermitteln, wie man mit (erkannten) Angriffen umgehen soll;
- Vermitteltes Wissen und gestellten Situationen trainieren;
- Anwenden des erlernten Wissens im Arbeitsalltag;
- Sicherheit als ein positives Thema begreifen und gemeinsam Beitrag leisten (Stichwort Sicherheitskultur).

Entsprechend ist es wichtig, dass Sie sich klar sind, welche Aspekte Sie mit Ihren Maßnahmen abdecken möchten.



EMPFEHLUNG 2: ERST TECHNISCHE MASSNAHMEN UND SECURITY POLICIES AUF DEN AKTUELLEN STAND BRINGEN

Ein adäquater Schutz vor Cyber-Angriffen ist nur dann möglich, wenn die technischen Schutzmaßnahmen ausgereizt sind, die Security Policies dem aktuellen Stand der Technik entsprechen und die verbleibenden Einfallstore durch geeignete Security Awareness-Maßnahmen adressiert werden. Beispielsweise sind die technischen Schutzmaßnahmen noch nicht ausgereizt, wenn:

- Betriebssystem und /oder Software nicht auf dem aktuellen Stand sind,
- Es kein funktionierendes Backup System gibt,
- Anhangstypen wie .exe in E-Mails nicht geblockt werden,
- (externe) USB-Geräte einfach verwendet werden können, oder
- Geräte nicht nach kurzer Zeit der Nicht-Benutzung automatisch gesperrt werden.

Beispielsweise ist Ihre Password Policy nicht auf dem aktuellen Stand der Technik, wenn diese verlangt, dass Passwörter regelmäßig geändert werden müssen. An dieser Stelle empfiehlt es sich auch zu prüfen, ob bereits genügend technische Unterstützung für die Umsetzung von Policies genutzt wird, z.B. Password Manager im Einsatz sind bzw. technische Unterstützungen zur Untersuchung von URLs hinter Links in E-Mails vorhanden sind. Es ist wichtig, dass die technischen Maßnahmen und Security Policies klar definiert sind und Ihnen bekannt ist, auf welche Annahmen an das Nutzerverhalten Sie beruhen, um dann genau dort mit den Security Awareness Maßnahmen anzusetzen.

EMPFEHLUNG 3: EINFÜHRUNG EINES FRAGE- BZW. MELDEWESENS FÜR INFORMATIONSSICHERHEIT

Gute Security Awareness Maßnahmen führen dazu, dass Ihre Kolleginnen und Kollegen aufmerksamer und vorsichtiger werden bzw. eher merken, wenn sie potentiell auf einen Angriff reingefallen sind oder sich unsicher verhalten haben. Daher ist es wichtig, dass vor dem Start der eigentlichen Security Awareness Maßnahme ein entsprechendes Frage- und Meldewesen eingerichtet und etabliert ist. Hierbei wird u.a. festgelegt,

- in welchen Fällen (inkl. Beispielen), Fragen gestellt werden können und sollen, an wen diese zu richten sind und welche Antwortzeiten (ggf. themenabhängig) angestrebt werden;
- welche Fälle zur Meldepflicht gehören, sowie an wen diese unmittelbar zu melden sind (falls weitere Aktionen gefordert sind, wie nur das Melden, ist auch dies zu definieren);
- wie mit Angriffen / Fehlverhalten umzugehen ist, die selbst bemerkt, abgewehrt bzw. korrigiert wurden.

Dabei ist es wichtig, dass die Fälle klar und verständlich definiert sind, was idealerweise evaluiert wird, bevor die Informationen später verteilt werden. Das Frage- und Meldewesen ist vom Anbieter her so zu gestalten, dass sich jemand, der sich meldet, nicht unwohl fühlt. Hierfür sind die betreffenden Personen beim Anbieter des Frage- und Meldewesens ggf. zu schulen.



Bevor die Prozesse in der Organisation kommuniziert werden, sollte überlegt werden, wie der Aspekt der Meldepflicht kommuniziert wird, so dass einerseits keine Angst davor entsteht andererseits aber verstanden wird, warum es wichtig ist hier mitzumachen¹. Bei der Kommunikation ist auch darauf zu achten, dass klar ist, dass mehr Informationen folgen und im Moment vor allem wichtig ist, sich der Unterschiede klar zu machen, zu wissen wen man fragt und dem Ansatz offen gegenübersteht dies einfach mal auszuprobieren. Zur Unterstützung des Merkens, können auch entsprechende Materialien verteilt werden, wie z.B. ein Sticker mit den Informationen für den Laptop oder den Monitor.

VERDÄCHTIGES VERHALTEN ERKENNEN

- Dein Browser öffnet ungefragt neue Webseiten, insbesondere Internetangebote fragwürdigen Inhalts oder zeigt auf bekannten Seiten viel mehr Werbung an, ggf. auch für fragwürdige Inhalte.
- Du bekommst Bestellbestätigungen, Stornierungsbestätigungen und/oder Mahnbescheide für ungetätigte Bestellungen. Verwende zur Klärung nicht die Links in E-Mail oder Brief, sondern gehe direkt auf die Seite des Shops.
- Dein Computer zeigt auf dem Bildschirm eine Statusmeldung an, dass er verschlüsselt wurde und nur noch gegen Zahlung von Lösegeld entsperrt werden kann.
- Bei Deinem Zahlungsdienstleister (z.B. Bankkonto, Paypal, etc.) sind Vorgänge zu sehen, die Du nicht genehmigt hast.
- Auf Deinem Rechner sind/werden Programme installiert, die vorher nicht da waren. Merkwürdige Fenster oder Anwendungen werden automatisch gestartet.
- Kollegen, Verwandte oder Bekannte sprechen Dich darauf an, dass sie von Dir merkwürdige E-Mails bekommen haben.

EMPFEHLUNG 4: DIE CHEF-ETAGE IST AN BOARD

Wie bei fast allen Maßnahmen in Organisationen, ist es auch hier wichtig, dass die Chefs hinter den Entscheidungen, Prozessen und Maßnahmen stehen, selbst daran teilnehmen und in Ihrer eigenen Kommunikation zeigen, wie wichtig Ihnen das Thema ist. Chefs, die Trainings selbst nicht machen und die Ausnahmeregelungen von den Security Policies haben sind kein Vorbild. Entsprechend schwieriger ist es, dass die Kolleginnen und Kollegen das Thema ernst nehmen.

¹ Müllmann/Volkamer, Meldepflicht von Mitarbeitenden bei IT-Sicherheits- und Datenschutzvorfällen - Betrachtung möglicher arbeitsrechtlicher Konsequenzen, ZD 2021

EMPFEHLUNG 5: INHALTLICHE AUSGESTALTUNG IM EINKLANG MIT ADRESSATEN, TECHNIK, ARBEITSABLÄUFEN UND SECURITY POLICIES

Bei der inhaltlichen Ausgestaltung ist zunächst wichtig, die Ausgangslage der Adressaten zu kennen – sprich welche Mentalen Modelle und welches Wissen haben diese in Bezug auf Informationssicherheit, wo brauchen sie Unterstützung und wie stehen sie allgemein zum Thema Informationssicherheit. Dies wird bedeuten, dass es unterschiedliche Maßnahmen für unterschiedliche Gruppen in der Organisation geben wird, zumindest bis alle etwa auf dem gleichen Stand sind. Die Inhalte sollten unbedingt im Einklang mit der eingesetzten Sicherheitstechnik und den Security Policies stehen (z.B. sollte das Passwort-Training nicht empfehlen, lieber sehr lange, statt sehr komplexe Passwörter zu verwenden, wenn Ihre Passwort-Policy acht Stellen vorsieht sowie die Verwendung von mindestens zwei Sonderzeichen, mindestens einer Zahl sowie mindestens einem Groß- und einem Kleinbuchstaben). Erklären Sie in Security Awareness Maßnahmen nicht, dass überall andere Passwörter zu verwenden sind, wenn Sie keinen Passwort Manager erlauben, aber wissen, dass einige Kolleginnen und Kollegen viele unterschiedliche Accounts für unterschiedliche Dienste benötigen. Achten Sie darauf, dass die vermittelten Inhalte konkret und die verschiedenen Angriffsarten abdeckt sind. Beispielsweise sollte nicht nur vermittelt werden, dass man wegen Phishing E-Mails vorsichtig mit Anhängen und Links sein soll, sondern erklärt werden, welche Kanäle für Phishing genutzt werden und woran man erkennen kann, dass das Öffnen eines Anhangs bzw. das Klicken eines Links gefährlich ist. Zahlreiche Studien² zeigen, dass Vorgaben bzgl. sicherem Verhalten, nur dann eingehalten werden, wenn die Self-Efficacy (Selbstwirksamkeit) mit Hinblick auf die Umsetzung dieses sicheren Verhaltens hoch ist.

Meist stellt sich auch die Frage, mit welchen Themen zu beginnen oder welche Themen zu priorisieren sind. Hier hilft eine Risikoanalyse, die verdeutlicht, welche Einfallstore über Kolleginnen und Kollegen das größte Risiko bürden. Dies kann auch von Bereich zu Bereich in der Organisation unterschiedlich sein. Idealerweise werden die Maßnahmen darauf angepasst.

EMPFEHLUNG 6: VIELFALT AN MEDIEN

Ihre Kolleginnen und Kollegen werden unterschiedliche Vorlieben für unterschiedliche Medien (eLearnings, Erläuterungen auf Webseiten, Video – Zeichentrick versus Interview versus nachgestellt, Serious Games – online oder offline; mit und ohne Möglichkeit gegeneinander anzutreten) haben. Security Awareness Maßnahmen sind am effektivsten, wenn für jeden was dabei ist. Das Thema Informationssicherheit sollte möglichst breit platziert werden. So sollte die Hauptmaßnahme möglichst mit kleinen Angeboten

erweitert werden: z.B. entsprechenden Give-Aways, thematisch passende Poster als Erinnerung oder als Challenge, das Wissen gerade auf die Probe zu stellen, Security-Stammtische für Beginners.

EMPFEHLUNG 7: MESSEN SIE DIE EFFEKTIVITÄT ODER BITTEN DEN ANBIETER VOR VERTRAGSABSCHLUSS ÜBER EINZUKAUFENDE SECURITY AWARENESS MASSNAHMEN IHNEN EINEN NACHWEIS HIERÜBER ZU GEBEN.

Nachdem die Vorbedingungen für effektive Security Awareness Maßnahmen durch die ersten vier Empfehlungen gegeben sind und Sie auch bei Inhalten und Ausgestaltung den Empfehlungen gefolgt sind, stehen die Chancen gut, dass die entwickelten Security Awareness Maßnahmen auch wirklich effektiv sind. Was mit „effektiv“ genau gemeint ist, hängt von dem definierten Ziel ab. Bevor Sie damit allerdings an alle Kolleginnen und Kollegen herantreten und diese dafür wertvolle Arbeitszeit investieren, sollte sichergestellt sein, dass die geplanten Maßnahmen auch wirklich effektiv sind. Dies kann entweder geschehen, weil Sie die Maßnahme erst für einzelne Kolleginnen und Kollegen evaluieren oder – im Fall, dass Sie die Maßnahmen einkaufen –, dass der Anbieter Ihnen einen Nachweis gibt, dass die Maßnahme in ähnlichen Organisationen effektiv mit Bezug zu den von Ihnen definierten Zielen war.

WEITERFÜHRENDE EMPFEHLUNGEN: WEITERE WICHTIGE THEMEN IN DIESEM ZUSAMMENHANG SIND

- Kolleginnen und Kollegen die Zeit für die Teilnahme an den Security Awareness Maßnahmen zu geben;
- Ihnen die Zeit im Arbeitsalltag für Security zu geben;
- das Auffrischen des Wissens nach einer gewissen Zeit – und nicht indem das gleiche Training einmal im Jahr durchlaufen werden soll; hierzu ist es nötig, die Effektivität auch über die Zeit beurteilen zu können; und
- das On-Boarding neuer Kolleginnen und Kollegen.

Die Ergebnisse, die in dieser Broschüre aufgeführt sind, wurden u.a. vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des KASTEL Projekts gefördert.

² EINISA: Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity (2018)

PARTNER



AUTOREN



PROF. DR. MELANIE VOLKAMER
Professorin für Security Engineering
Karlsruher Institut für Technologie

@ Melanie.Volkamer@kit.edu



BENJAMIN BACHMANN
Director Cyber Security
EXXETA

@ Benjamin.Bachmann@exxeta.com