EXXETA
CONSULTING AND TECHNOLOGIES

SECURITY SENSIBILISIERUNG FÜR BESCHÄFTIGTE

EMPFEHLUNGEN FÜR INFORMATIONS-SICHERHEITSBEAUFTRAGTE

KIT Karlsruher Institut für Technologie
aifb
SECUSO SECURITY · USABILITY · SOCIETY
KD²lab Decision&Design
KASTEL

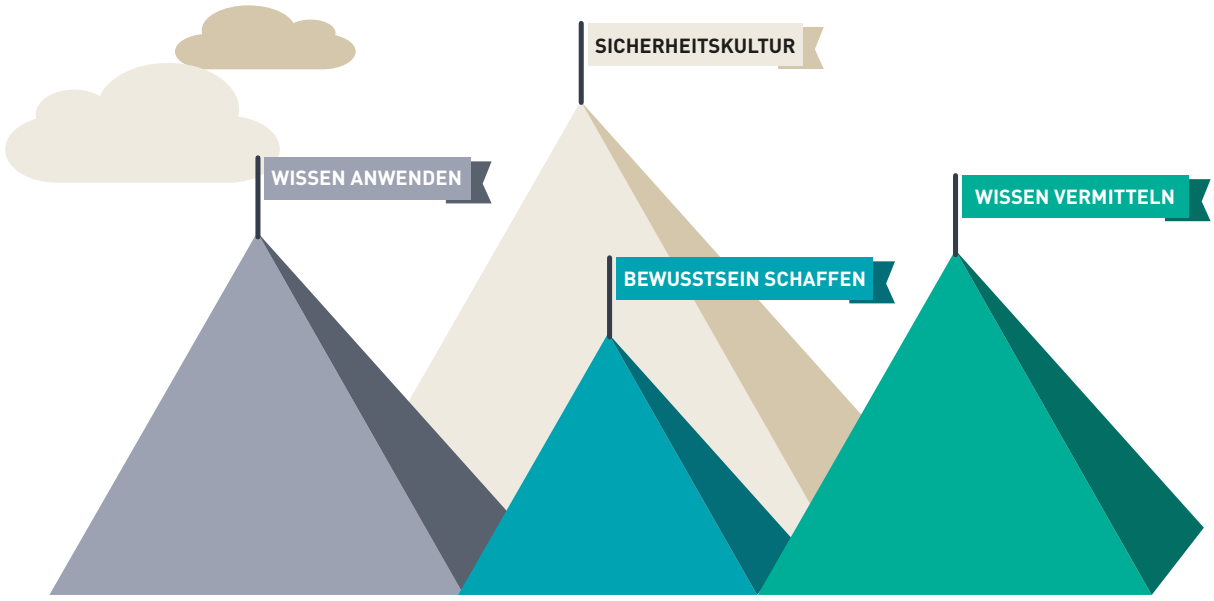
Sie sind Informationssicherheitsbeauftragte(r) und haben daher die Aufgabe, Ihre Kolleginnen und Kollegen, deren primäres Ziel nicht Informationssicherheit ist, für das Thema zu sensibilisieren? Dann haben wir in diesem Beitrag einige Tipps und Empfehlungen – aus der Praxis und der Wissenschaft – zur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

EMPFEHLUNG 1: ZIEL FESTLEGEN

Es existieren verschiedene Security Awareness-Maßnahmen wie z. B.:

- Bewusstsein für Angriffe schaffen;
- Bewusstsein dafür 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 zu sicherem Verhalten in gestellten Situationen vertiefen bzw. trainieren;
- Anwenden des erlernten Wissens im Arbeitsalltag;
- IT-Sicherheit als ein wichtiges Thema begreifen und gemeinsam Beitrag leisten (Stichwort Sicherheitskultur).

Entsprechend ist es wichtig, dass Sie sich klar darüber 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 - u. a. weil bei den Endgeräten Updates nicht automatisch eingespielt werden,
- 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 bzw. technische Unterstützung zur Untersuchung von Links in E-Mails. Es ist wichtig, dass die technischen Maßnahmen und Security Policies klar definiert sind und Ihnen bekannt ist, auf welchen 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-Maßnahmen 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 außer der Meldung noch weitere Aktionen gefordert sind), z. B. ob das Gerät unmittelbar ausgeschaltet werden soll und / oder vom Internet getrennt werden soll
- 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, sich nicht unwohl fühlt. Bei Bedarf sind die betreffenden Personen vom Anbieter des Frage- und Meldewesens zu schulen.

Bevor die Prozesse in der Organisation eingeführt werden, sollten IT-Sicherheitsbeauftragte die Inhalte der Meldepflicht klar kommunizieren. Einerseits sollen sie den Beschäftigten Ängste davor nehmen andererseits müssen sie verständlich machen, warum es wichtig ist hier mitzumachen[1]. Bei der Kommunikation ist klarzustellen, dass mehr Informationen folgen und es im Moment vor allem wichtig ist, zu wissen wen man fragt und dem Ansatz offen gegenübersteht, dies einfach mal auszuprobieren. Zur Unterstützung von Telefonnummern oder E-Mail Adressen, können Materialien verteilt werden, wie z. B. ein Sticker mit den Informationen für den Laptop oder den Monitor.

EMPFEHLUNG 4: DIE CHEFETAGE IST AN BOARD

Wie bei fast allen Maßnahmen in Organisationen, ist es auch hier wichtig, dass die Geschäftsleitung hinter den Entscheidungen, Prozessen und Maßnahmen stehen, selbst daran teilnehmen und in Ihrer eigenen Kommunikation zeigen, wie wichtig Ihnen das Thema ist. Führungskräfte, die Trainings selbst nicht machen und die Ausnahmeregelungen von den Security Policies haben, sind

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

kein Vorbild. Entsprechend schwieriger ist es, dass die Kolleginnen und Kollegen das Thema ernst nehmen.

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

Bei der inhaltlichen Ausgestaltung ist es 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 bedeutet, 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 Passwortmanager 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. Vermitteln Sie beispielsweise nicht nur, dass man wegen Phishing E-Mails vorsichtig mit Anhängen und Links sein soll, sondern erklären Sie, welche Kanäle für Phishing genutzt werden und woran man erkennen kann, dass das Öffnen eines Anhangs bzw. das Klicken eines Links gefährlich ist. Zahlreiche Studien[2] 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 ist oder welche Themen zu priorisieren sind. Hier hilft eine Risikoanalyse, die verdeutlicht, welche Einfallstore das größte Risiko bergen. Dies kann 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 haben (eLearnings, Erläuterungen auf Webseiten, Video – Zeichentrick versus Interview versus nachgestellt, Serious Games – online oder offline; mit und ohne Möglichkeit gegeneinander anzutreten). Security Awareness-Maßnahmen sind am effektivsten, wenn für jeden etwas dabei ist. Das Thema Informationssicherheit sollte möglichst breit platziert werden, so sollte die Hauptmaßnahme möglichst mit kleinen Angeboten erweitert werden: z. B. Give-Aways, thematisch passende Poster als Erinnerung oder als Challenge[3], das Wissen gerade auf die Probe zu stellen, Security-Stammtische für Anfänger.

EMPFEHLUNG 7: MESSEN SIE DIE EFFEKTIVITÄT ODER FRAGEN SIE VOR VERTRAGSABSCHLUSS UND KAUF DER SECURITY AWARENESS-MASSNAHMEN NACH EINEM EFFEKTIVITÄTSNACHWEIS.

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 die Effektivität der Maßnahmen sichergestellt sein. 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 Maßnahmen in ähnlichen Organisationen effektiv mit Bezug zu den von Ihnen definierten Zielen war.

WEITERFÜHRENDE EMPFEHLUNGEN: WEITERE WICHTIGE THEMEN IN DIESEM ZUSAMMENHANG SIND & MOTIVATION DER MITARBEITER NICHT ÜBERSTRAPAZIEREN UND HOCHHALTEN.

- Kolleginnen und Kollegen die Zeit für die Teilnahme an den Security Awareness-Maßnahmen zu geben;
- die Beweggründe der MitarbeiterInnen, sich für Informationssicherheit zu engagieren, berücksichtigen, um deren Motivation nicht überzustrapazieren und hochzuhalten;
- 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 Borschüre 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)
[3] https://secuso.aifb.kit.edu/Poster_Phishing_BetrNachrichten.php

PARTNER

Karlsruher Institut für Technologie

AUTOREN

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

@ **Melanie.Volkamer@kit.edu**

BENJAMIN BACHMANN
Director Cyber Security
EXXETA AG

@ **Benjamin.Bachmann@EXXETA.com**

Stand: März 2021/ Version 1.1