Dialog für Cyber-Sicherheit

Empfehlungen für die Entwicklung und Evaluation von Security-Awareness-Maßnahmen:

Leitfaden des Workstreams „Effektive IT-Security-Awareness: Wirksam ein Bewusstsein für Risiken schaffen ”

Stand: 04.05.2022

Informationen zum Produkt

Dieser Leitfaden wurde im Rahmen des Projekts „Dialog für Cyber-Sicherheit“ von Juli 2021 bis April 2022 erarbeitet.

Ideengeber:innen des Workstreams waren:
Martina Angela Sasse, Ruhr-Universität Bochum
Melanie Volkamer, Karlsruher Institut für Technologie (KIT), Forschungsgruppe SECUSO

Mitwirkende Teilnehmer:innen des Workstreams waren:
Nadja Menz, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Simon Trang, Georg-August-Universität Göttingen
Steffen Hessler, Ruhr-Universität Bochum
Michael Große, Informationstechnikzentrum Bund
Cedric Mössner, Morpheus Tutorials
Ayten Öksüz, Verbraucherzentrale NRW
Ines Schieferdecker, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Beteiligte Mitarbeiter:innen der Geschäftsstelle (iRights.Lab) waren:
Jörg Rodermund
Viktar Vasileuski
Vera Dünninger
Marcel Schneuer
Wiebke Glässer

Lektorat:
Hannah Willing

Der Dialog für Cyber-Sicherheit ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das vom Think Tank iRights.Lab und dem nexus Institut durchgeführt wird. Die Auftragnehmer haben dazu eine Geschäftsstelle eingerichtet.

Der Workstream „Effektive IT-Security Awareness: Wirksam ein Bewusstsein für Risiken schaffen“, in dem der Leitfaden entstanden ist, wurde im Rahmen eines partizipativen und offenen Austauschs von der Geschäftsstelle (iRights.Lab) und interessierten Dialogpartner:innen (s. Ideengeber:innen und mitwirkende Teilnehmer:Innen) durchgeführt. Die Dialogpartner:innen haben das Thema aus dem Bereich Cyber-Sicherheit für den Workstream selbst gewählt.

Der vorliegende Leitfaden wurde von der Geschäftsstelle und den Workstream-Teilnehmer:innen eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. jedes einzelnen Teilnehmenden wider. Das BSI verfolgt mit dem Projekt das Ziel, einen offenen gesellschaftlichen Diskurs zum Thema IT-/Cyber-Sicherheit sowie damit verwandter gesellschaftlicher Themen zu ermöglichen. Das Projekt soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung

an das Thema Cyber-Sicherheit aus Sicht der Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Weitere Informationen zum „Dialog für Cyber-Sicherheit“:
www.dialog-cybersicherheit.de
Kontakt Geschäftsstelle (iRights.Lab und nexus Institut):
kontakt@dialog-cybersicherheit.de

Stand: April 2022

iRights.Lab
Think Tank für die digitale Welt

nexus

Ein Projekt im Auftrag des:
Bundesamt für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

1. Einleitung

Dieser Leitfaden ist das Ergebnis des Workstreams 4 „Effektive IT-Security-Awareness: Wirksam ein Bewusstsein für Risiken schaffen“, der im Rahmen des Projekts „Dialog für Cyber-Sicherheit“ im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) entstanden ist.

Von Juli 2021 bis März 2022 haben es sich die Teilnehmer:innen des Workstreams zur Aufgabe gemacht, Security-Awareness-Maßnahmen unter Einbindung aktueller wissenschaftlicher Erkenntnisse zu erstellen. Im Fokus stehen Maßnahmen, die unterschiedliche Gruppen von Verbraucher:innen adressieren. Die fachlich-wissenschaftliche Expertise wurde durch die Sessionpatinnen Prof. Dr. Melanie Volkamer und Prof. Dr. Martina Angela Sasse bereitgestellt. Aufgrund diverser Rahmenbedingungen ist deren Expertise jedoch erst am Ende der Bearbeitungszeit eingeflossen, so dass die Einbindung der übrigen Teilnehmenden des Workstream erst in den letzten Treffen erfolgt ist und der geplante Dialog zwischen den Beteiligten nur in sehr eingeschränktem Maß stattfinden konnte.

Die folgenden Schritte sollen Ersteller:innen von Awareness-Maßnahmen dabei helfen, diese so auszugestalten, dass sie für die Anwender:innen effektiv sind. Hierbei handelt es sich nicht um einen linearen, sondern um einen iterativen Vorgehensvorschlag. Es kann notwendig sein, aufgrund der Ergebnisse von Prozessschritten zu vorherigen Schritten zurückzukehren.

2. Fünf Schritte für die Entwicklung und Evaluation von Security-Awareness-Maßnahmen

2.1 Definition der Zielgruppe

Unterschiedliche Zielgruppen für Awareness-Maßnahmen nutzen unterschiedliche IT (Hardware, Betriebssysteme, Software/Apps, Internetdienste) und IT-Sicherheits-maßnahmen. Bei den Zielgruppen sind das Bewusstsein für IT-Security-Risiken sowie die Bedeutsamkeit, sich mit dem Thema IT-Security zu beschäftigen, ungleich stark ausgeprägt. Die Zielgruppen verfügen über variierende Fähigkeiten und – gegebenenfalls sogar falsche – Vorstellungen davon, welche Gefahren relevant sind und welche Maßnahme welchen Schutz bieten kann. Zudem sind die verschiedenen Zielgruppen mit ihren voneinander abweichenden Lebenskontexten nicht immer über die gleichen Kanäle zu erreichen. Darüber hinaus bevorzugen die jeweiligen Zielgruppen verschiedene Formate der Security-Awareness-Maßnahmen (z. B. Video, Spiel oder Vortrag). Zuletzt sei erwähnt, dass die Zielgruppen ungleichmäßig viel Zeit in die Maßnahmen investieren können.

Es ist wichtig, dass die Zielgruppe einer Awareness-Maßnahme von den Ersteller:innen eindeutig definiert und verstanden wird.

Einige der genannten Aspekte können je nach Thema und Ziel der IT-Security-Awareness-Maßnahme voneinander abweichen. Entsprechend sind die ersten beiden Schritte eng miteinander verzahnt.

2.2 Definition der Zielsetzung

IT- bzw. Informationssicherheit umfasst sehr viele Aspekte. Für eine einzelne IT-Security-Awareness-Maßnahme wird daher in der Regel ein konkretes Thema ausgewählt (z. B. der Schutz von Benutzer:innenkonten). Entsprechend sind die Beispiele in diesem Kapitel an das jeweilige Thema anzupassen.

Es existieren verschiedene Definitionen des Begriffs IT-Security-Awareness. Daher können auch unterschiedliche Ziele mit einer Awareness-Maßnahme verfolgt werden. Im Folgenden werden – sowohl aus der Forschung als auch aus der Praxis – typische Ziele von IT-Security-Awareness-Maßnahmen zusammengestellt (auch Kombinationen sind möglich):

- Adressat:in ist motiviert, sich weiterhin mit dem Thema (das Thema ist zu benennen) zu beschäftigen.

- Adressat:in ist sich der Gefahren inklusive möglicher Konsequenzen (d. h., warum es wichtig ist, sich zu schützen) bewusst (die Gefahren und potenziellen Konsequenzen sind zu benennen): Die Adressat:in ist sich nicht nur bewusst, dass es diese gibt, sondern auch, dass sie betroffen ist.
- Adressat:in erfährt, wie (un)sicheres Verhalten aussieht ([un]sicheres Verhalten ist zu benennen).
- Adressat:in erfährt, wie (un)sicheres Verhalten aussieht und welches sichere Verhalten vor welchen Gefahren schützt (die Gefahren mit realen Beispielen und das [un]sichere Verhalten sind zu benennen).
- Adressat:in erfährt, wie sicheres Verhalten aussieht, und ist überzeugt, dass dieses vor konkreten Gefahren schützt (die Gefahren und das sichere Verhalten sind zu benennen).
- Adressat:in hat das Gefühl, das sichere Verhalten im Alltag umsetzen zu können (sicheres Verhalten ist zu benennen).
- Adressat:in erfährt, wie sicheres Verhalten aussieht, und setzt dieses im Alltag um (sicheres Verhalten ist zu benennen).
- Adressat:in führt sicheres Verhalten – nach der Maßnahme/ dauerhaft – eigenständig und automatisiert im Alltag durch (sicheres Verhalten ist zu benennen).
- Adressat:in verringert falsche Vorstellungen von den relevanten Gefahren und der Wirksamkeit konkreter Maßnahmen (die Gefahren und das sichere Verhalten sind zu benennen).

Es ist wichtig, dass die Ziele für IT-Security-Awareness-Maßnahmen zu Beginn des Entwicklungsprozesses präzise definiert werden*.*

2.3 Festlegung der Inhalte

In Abhängigkeit vom definierten Ziel und der definierten Zielgruppe ist der Inhalt der jeweiligen IT-Security-Awareness-Maßnahme festzulegen.

Zunächst sollten Gefahren mithilfe einer Bedrohungs- bzw. Risikoanalyse für die Zielgruppe identifiziert werden. Eine Analyse der relevanten Literatur kann dabei helfen, keine relevanten Gefahren zu übersehen. Wenn im Rahmen der Analyse Gefahren identifiziert werden, die nicht in die Maßnahme integriert werden können bzw. sollen, sollte dies zum Zweck der Nachvollziehbarkeit dokumentiert werden.

Es ist wichtig, dass die adressierten Gefahren für die Zielgruppe relevant sind, also ein hohes Risiko darstellen.

Wenn die IT-Security-Awareness-Maßnahmen ergänzend Empfehlungen für die Zielgruppe (im Sinne des sicheren Verhaltens) enthalten sollen, dann sollte zum Zweck der Nachvollziehbarkeit dokumentiert werden, inwieweit diese Empfehlungen den zuvor identifizierten Gefahren zugeordnet werden und einen adäquaten Schutz vor ihnen bieten können.

Es ist wichtig, dass die Empfehlungen dem aktuellen Stand der BSI-Empfehlungen sowie der wissenschaftlichen Literatur entsprechen.

Die Empfehlungen sollten so konkret dargestellt werden, dass die Zielgruppe nachvollziehen kann, wie diese im Alltag umzusetzen sind. Die Aussage „Es ist wichtig, sein Nutzer:innenkonto zu schützen“ ist – ohne eine Erläuterung der konkreten Umsetzung – keine wirksame Empfehlung.

Es ist wichtig, dass die Empfehlungen, die in den IT-Security-Awareness-Maßnahmen enthalten sind, für die jeweilige Zielgruppe anwendbar sind.

2.4 Festlegung des Formats und der Sprache

Das Format, in dem die Inhalte umgesetzt werden, hängt von den Inhalten und den Zielgruppen ab. Hierbei ist auch zu klären, ob die Inhalte alle in einer IT-Security-Awareness-Maßnahme thematisiert werden können oder ob es zielführender ist, die Inhalte auf mehrere Maßnahmen aufzuteilen.

Die sprachliche/bildliche Vermittlung der Inhalte sollte zielgruppengerecht ausgewählt werden. Es empfiehlt sich eine Orientierung an Konzepten der sogenannten „Einfachen Sprache“, um die Inhalte verständlich zu vermitteln und keine (sprachlichen) Hürden aufzubauen. Hürden könnten beispielsweise die Nutzung von Fachsprache sowie die Verwendung von Fachbegriffen in englischer Sprache sein.

Es ist wichtig, ein geeignetes Format für den jeweiligen Inhalt und die jeweilige Zielgruppe auszuwählen. Zudem muss darauf geachtet werden, dass die sprachliche Formulierung/ bildliche Darstellung zielgruppengerecht erfolgt.

2.5 Evaluation: Wird das gesetzte Ziel erreicht?

Die jeweilige Zielgruppe weiß am besten, ob Format und Sprache für sie geeignet sind. Daher sollten einige repräsentative Vertreter:innen der Zielgruppen in den Entwicklungsprozess eingebunden werden. In einer frühen Phase können gemeinsam (auch auf den ersten Blick

abwegige) Ideen gesammelt und diskutiert werden. Zudem sollten Format und Sprache evaluiert und basierend auf den gewonnenen Erkenntnissen verbessert werden. Hierzu könnten beispielsweise Fokusgruppen eingesetzt werden.

Es ist wichtig, Personen aus der Zielgruppe in den Entwicklungsprozess einzubeziehen.

Es ist essenziell, dass die IT-Security-Awareness-Maßnahme vor ihrer Verbreitung mit einem möglichst repräsentativen Personenkreis der Zielgruppe abschließend evaluiert wird. Mittels einer entsprechenden Nutzer:innenstudie wird gezeigt, dass das gesetzte Ziel für die identifizierte Zielgruppe mit der entwickelten IT-Security-Awareness-Maßnahme erreicht wird. Bei der Evaluation muss man sich vor Augen führen, dass die Evaluation der Maßnahme und nicht der Teilnehmenden im Mittelpunkt steht. Dies muss bei der Kommunikation mit den Teilnehmenden beachtet werden.

Bei der Ausgestaltung der empirischen Studie muss für jedes Ziel festgelegt werden, wie gemessen werden soll, dass das Ziel erreicht wurde. Hierfür sind im ersten Schritt geeignete Messpunkte festzulegen. Messpunkte sind notwendige Bedingungen für die Zielerreichung. Ist das übergreifende Ziel einer Maßnahme beispielsweise die Sensibilisierung der Adressat:in für die Gefahren von Phishing-E-Mails, könnten sich geeignete Messpunkte auf Kenntnisse zu deren Wahrscheinlichkeit (Wie wahrscheinlich sind Phishing-Angriffe?) und deren Gefahrenpotenzial (Welche schwerwiegenden Konsequenzen können Phishing-Angriffe haben?) beziehen. Ist das Ziel einer Maßnahme der sichere Umgang mit (Phishing-)E-Mails, könnte ein Messpunkt die signifikante Steigerung der Erkennungsrate von Phishing-E-Mails sein. Im zweiten Schritt sind geeignete Instrumente auszuwählen, z. B. ein Quiz oder eine Laborstudie. Bei der Durchführung ist unter anderem darauf zu achten, dass ethische und datenschutzrechtliche Vorgaben eingehalten werden.

Es ist wichtig, für jedes Ziel mindestens einen Messpunkt festzulegen. Zudem müssen für jeden Messpunkt adäquate Messinstrumente ausgewählt werden.

3. ANHANG

Evaluationsbeispiel: Social Engineering bei Senior:innen

Bedrohung (Gefahren und mögliche Konsequenzen):

Senior:innen werden bei Social Engineering per Telefon angegriffen: Eine angebliche Mitarbeiterin von „Microsoft Support" ruft an, um über eine Schwachstelle zu informieren, bietet Hilfe beim Schließen der Schwachstelle an, lässt sich zu diesem Zweck einen Fernzugriff einrichten und hat nun Zugang zu dem Computer. Durch dieses Vorgehen können Kriminelle alle Funktionen, Dienste und Daten des Rechners ebenso wie die Eigentümer:innen nutzen (z. B. Dateien verändern, löschen, veröffentlichen, E-Mails verschicken). Zusätzlich können die Kriminellen die Daten verschlüsseln, um die Eigentümer:innen der Computer zu erpressen.

Ziel der Awareness-Maßnahme:

1. Adressat:in ist sich der Gefahren inklusive möglicher Konsequenzen bewusst (Gefahren und potenzielle Konsequenzen siehe 2.) – nicht nur, dass es diese gibt, sondern auch, dass er/ sie betroffen ist.
2. Adressat:in erfährt, wie (un)sicheres Verhalten aussieht (sicheres Verhalten: Telefongespräch beenden; unsicheres Verhalten: sich in ein Gespräch verwickeln lassen, Herausgabe von Informationen).
3. Adressat:in hat das Gefühl, das sichere Verhalten im Alltag umzusetzen (sicheres Verhalten: Telefongespräch beenden; Stichwort Selbstwirksamkeit).
4. Adressat:in führt – nach der Maßnahme – sicheres Verhalten eigenständig und automatisiert im Alltag durch (sicheres Verhalten: Telefongespräch beenden).

Zielgruppe (Auswahl)**:** Senior:innen mit Windows-Rechnern mit Internetzugang und entsprechenden Administrations-Rechten sowie im Besitz eines Telefons.

IT-Security-Awareness-Maßnahme (grundsätzliche Idee)**:** Erstellung eines Videos, in dem die Gefahrensituation von Schauspieler:innen nachgestellt und von einer Kriminalbeamtin erklärt wird. Am Ende des Videos wird erläutert, wie man auf einen solchen Anruf reagiert (Telefongespräch beenden) und welche Fehler man vermeiden sollte (sich in ein Gespräch verwickeln lassen, Informationen herausgeben).

Abschließenden Evaluation: Werden die Ziele der Maßnahme erreicht?

Die Evaluation für Ziel 1 und 2 kann mit einem Wissensquiz erfolgen. Für das 3. Ziel existieren Fragen, die zur Messung der Selbstwirksamkeit genutzt werden können.

Für eine objektive Messung der Effektivität bezüglich des 4. Ziels müsste eine Bedrohung simuliert und gemessen werden, ob Teilnehmer:innen das Gespräch zügig beenden, ohne

Informationen herauszugeben. Solche Studien wären aufwendig und es müsste sichergestellt werden, dass sie ethisch zulässig sind. Ohne Studie ist eine Aussage hinsichtlich des vierten Ziels allerdings nicht möglich.