STRONG MINDS

CYBER RESILIENCE

BOTSCHAFTEN UND LERNZIELE IN SECURITY AWARENESS KAMPAGNEN

ANNE LAHNER

STRONG MINDS

CYBER RESILIENCE

Wenn wir mit einer Security Awareness Kampagne starten, soll natürlich sichergestellt sein, dass das letztlich auch etwas bringt. Die Anwender also die richtigen Botschaften bekommen, die dann zu einer Verhaltensänderung führen oder bestehendes sicheres Verhalten bestärken. Aber wie kommt man zu den richtigen Botschaften? Hier der Weg wie ich ihn gehe:

STRONG MINDS

1/7

WAS SOLLEN DIE USER KÖNNEN?

Awareness-Maßnahmen funktionieren nur, wenn wir klare Ziele verfolgen:

Welche Risiken sind am dringendsten?

Beispiel: Schwache Passwörter oder Passwort-Mehrfachverwendung.

Welches Verhalten möchten wir ändern?

Beispiel: Die Nutzung unsicherer Passwörter.

Welches Verhalten wollen wir etablieren?

Beispiel: Starke Passwörter, Passwort-Manager und MFA.

Können die User erklären, warum das wichtig ist?

→ Ziel ist nicht nur „Verständnis", sondern die Fähigkeit, zu erklären und zu handeln.

STRONG MINDS

2/7

RISIKEN PRIORISIEREN

Klar, hätten wir am liebsten, unsere User würden alles wissen hinsichtlich Security.
Um Awareness-Maßnahmen effektiv zu gestalten, müssen wir die Risiken priorisieren, die für unser Unternehmen den größten Einfluss haben (mal mit 10 Risiken anfangen!).
Beispiel:
Risiko: Schwache oder mehrfach verwendete Passwörter.
Ziel: Nutzer sollen starke Passwörter erstellen und Passwort-Safes sowie MFA nutzen.
Warum ist das entscheidend?
Weil genau hier eine Verhaltensänderungen das Risiko spürbar reduzieren kann.

STRONG MINDS

3/7

BOTSCHAFT ENTWICKELN

Also, hier stehen wir:

Das Problem:
Viele nutzen einfache, unsichere Passwörter und verwenden sie mehrfach.

Unser Ziel:

- Nutzer erstellen starke Passwörter.
- Sie setzen Passwort-Manager ein.
- Sie aktivieren MFA.

STRONG MINDS

4/7

LERNZIELE

Es reicht nicht, dass User etwas verstehen – sie müssen es anwenden können:

- Sie können erklären, warum starke Passwörter wichtig sind.
- Sie wissen, wie MFA funktioniert und warum es sie schützt.
- Sie können eigenständig einen Passwort-Manager nutzen.

Tipp: Lernziele sollten immer messbar sein. Die Frage lautet: Können die User zeigen, dass sie das Gelernte anwenden?

STRONG MINDS

5/7

VOM WISSEN ZUR PRAXIS

Awareness muss verständlich und praktisch sein. Anstatt nur Regeln zu verteilen, helfen wir mit klaren und nützlichen Lösungen:

Passphrasen statt Regeln:
Beispiel: „6Puddingschnecken&3Semmel'n" – leicht zu merken und sicher! Das geht weg von diesen scheußlichen Merksätzen, aus denen man die Anfangsbuchstaben etc. entnimmt.

Passwort-Manager nutzen:
Zeige Schritt für Schritt, wie ein Passwort-Manager eingerichtet wird. Unterstütze die User dabei, ihn zu lieben!

STRONG MINDS

6/7

ERFOLG MESSEN

Ok, Messung in der Kampagne ist noch mal ein eigenes dickes Thema, aber auch bei Lernzielen können wir messen:
Wie erkennen wir, dass unsere Maßnahmen erfolgreich sind?
Verhaltensänderungen:

- Mehr MFA-Nutzer
- Breitere Nutzung von Passwort-Managern (Downloadzahlen)
- Weniger schwache Passwörter.

Positives Feedback:

- „Das ist ja viel einfacher!“
- „Der Passwort-Safe ist ein Segen!“

Das Ergebnis:
Der User ist zufrieden, fühlt sich unterstützt und wendet das Gelernte aktiv an. So haben wir unser Ziel erreicht: Sicherheit wird selbstverständlich.

STRONG MINDS

7/7

FAZIT

So entwickeln wir effektive Botschaften
Zusammenfassung der wichtigsten Schritte:

1. Priorisiere die dringlichsten Risiken.
2. Definiere konkrete Lernziele.
3. Entwickle Botschaften, die Verhalten fördern – nicht nur Wissen vermitteln.
4. Biete praktische Lösungen an, die den Alltag erleichtern.
5. Miss den Erfolg anhand von Verhalten und Feedback.