Ihr Spezialist für Informationssicherheit

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

# Konzept Awareness

Awareness-Maßnahmen müssen, damit sie funktionieren, mehrere Bedingungen erfüllen.

1. Sie müssen die Lebensrealität der Mitarbeiter abbilden
2. Sie müssen interessant, ansprechend und verständlich sein
3. Sie müssen wiederholt werden, um eine regelmäßige Übung zu erreichen

In der Praxis muss deshalb eine Vielzahl verschiedener Punkte beachtet werden. Das folgende Konzept ist ein Vorschlag zum Erreichen sowie zur Aufrechterhaltung einer angemessenen Awareness.

### Baustein 1: Awareness Kampagne

Als erster Baustein wird eine insgesamt kleine Awareness Kampagne aufgesetzt, die einen ersten Hinweis auf Risiken für die Informationssicherheit gibt. Geeignet wäre beispielsweise eine einfache Poster-Kampagne mit zwei oder drei verschiedenen Postern zum Thema Phishing und Ransomviren. Diese Poster werden an sichtbaren und erkennbaren Stellen im Unternehmen aufgehängt und sollen erstmal einfach nur wahrgenommen werden.

### Baustein 2: Awareness Seminare

Als zweiter Baustein werden Awareness Seminare mit einem echten Trainer entweder als Video- oder als Präsenztraining aufgesetzt. Wir empfehlen drei Awareness Seminare für unterschiedliche Zielgruppen je nach Gefährdung im Unternehmen.

**1. Allgemeine IT-User**
Allgemeine IT-User sind Mitarbeiter die einen PC-Arbeitsplatz haben, insgesamt jedoch verhältnismäßig wenig gefährdet sind. Das sind üblicherweise Mitarbeiter mit Verwaltungstätigkeiten, die nicht direkt im Kundenkontakt stehen und nicht besonders exponiert sind.

**2. Exponierte IT-User**
In diese Gruppe fallen Mitarbeiter mit PC-Arbeitsplätzen, die besonders gefährdet sind. Das sind überwiegend Mitarbeiter die direkte Kundenkontakte besitzen und deshalb Ziel von Social Engineering Angriffen werden können. Außerdem Mitarbeiter die z.B. per Mail gesendete Rechnungen und Bewerbungen entgegennehmen, in denen Schadcode enthalten sein kann.

**3. Administratoren**
In die dritte Gruppe fallen alle Mitarbeiter die über Administratorrechte im Unternehmen verfügen und deshalb besondere Kenntnisse über die Gefährdungslage besitzen sollten.

In alle Seminare werden Screenshots und Bilder realer Phishing-Mails und Vorfälle im Unternehmen aufgenommen. Insbesondere wird die Awareness Kampagne in den Awareness Seminaren aufgegriffen, um eine Verknüpfung zwischen den verschiedenen Maßnahmen herzustellen.

Für diese drei Gruppen werden unterschiedliche Programme aufgesetzt:

| Gruppe | Inhalt | Dauer | Anzahl |
|---|---|---|---|
| Allgemeine IT-User | Kenntnis der internen Informationssicherheits-Richtlinien und der Meldepflichten bei Vorfällen. Allgemeine Erkennung von Phishing und Malware E-Mails, sichere Passwörter, Verhalten in sozialen Netzen, böse USB-Sticks. | 2 h | 25-30 User pro Gruppe |
| Exponierte IT-User | Exponierte IT-User benötigen mehr Kenntnisse insbesondere zur zuverlässigen Erkennung von Phishing- und Malware-Angriffen. Insbesondere sollten hier mehr Beispiele zur Vertiefung der Thematik aufgenommen werden. | 4 h | 15-20 User pro Gruppe |
| Administratoren | Administratoren sollen eine übergreifende Kenntnis von potentiellen Sicherheitsrisiken, Gefährdungen für das Unternehmen und richtigem Verhalten auch außerhalb ihres Spezialbereichs kennen. | 6 h | 10-15 User pro Gruppe |

Durch inhaltlich und zeitlich angepasste Inhalte an verschiedene Gruppen kann die Awareness Schulung sowohl zeitlich als auch preislich optimiert werden.

### Baustein 3: Awareness Test

Zur Vertiefung der Awareness Seminare sollte nach den Seminaren ein Awareness Test durchgeführt werden. Der Test sollte nicht nur Multiple Choice Fragen enthalten, sondern auch die Erkennung von Phishing-Mails, welche Indikatoren darauf hinweisen etc.
Idealerweise wird dafür entweder eine bereits vorhandene Lernplattform im Haus genutzt oder eine Inhouse-Lernplattform aufgebaut, die auch in Zukunft genutzt wird und die Teilnahme an Tests sowie an Online-Seminaren protokolliert und nachweist. Die jeweiligen Vorgesetzten sollten ihre Mitarbeiter anhalten, an den Tests tatsächlich teilzunehmen.

### Baustein 4: Social Engineering Angriffe

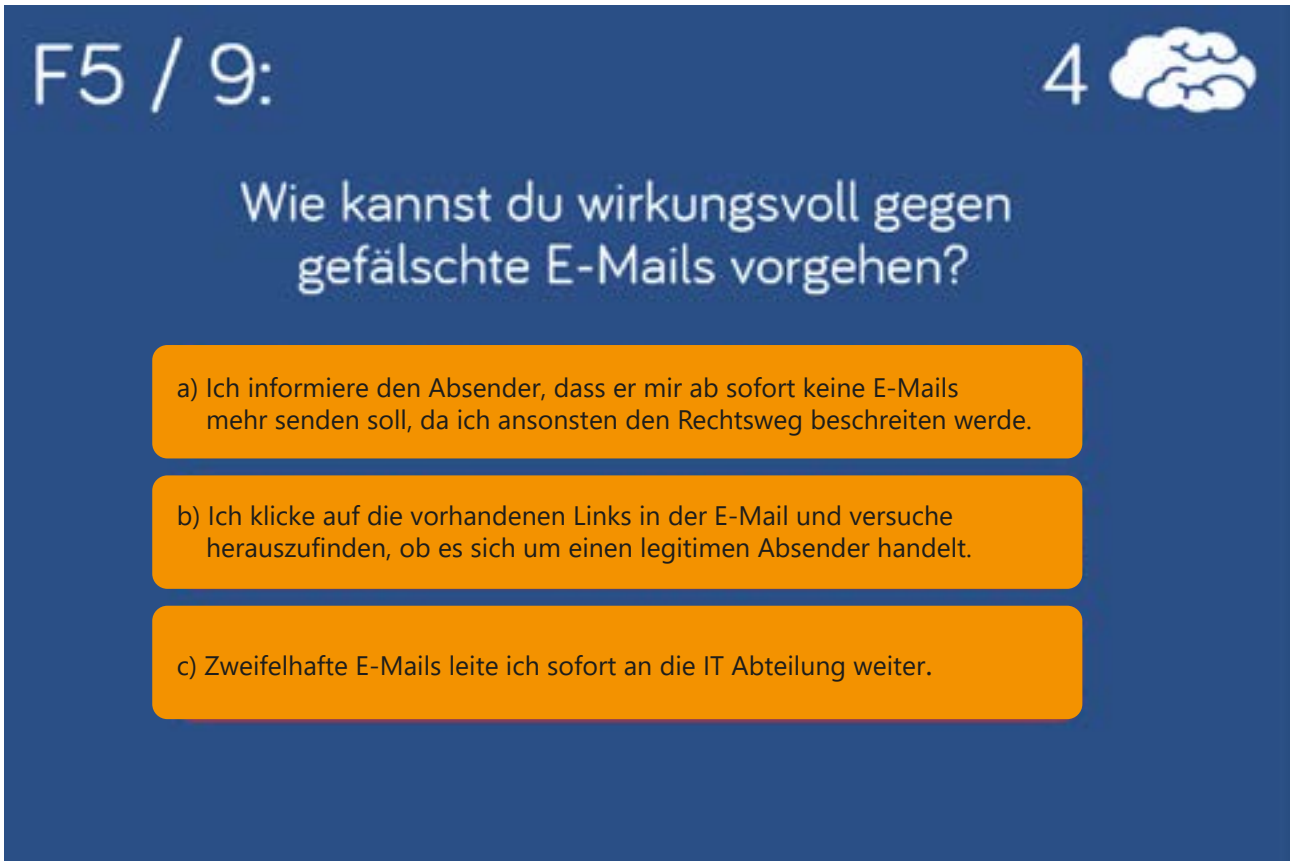
Mit einigen Monaten zeitlichem Abstand können dann Social Engineering Angriffe durchgeführt werden. Hier bieten sich für unterschiedliche Zielgruppen auch verschiedene Kampagnen an:

- **Social Engineering Angriff 1: Link zum Anklicken**
  - Webseite protokolliert, welche Anwender den Link geklickt haben
  - Weiterleitung auf das Lernportal zur Vertiefung der Kenntnisse der Mitarbeiter

- **Social Engineering Angriff 2: Phishing-Angriff**
  - E-Mail verspricht spezielle Vergünstigungen nur für Mitarbeiter
  - Anmeldung an spezieller Webseite mit Firmenlogin und Firmenpasswort notwendig
  - Weiterleitung auf das Lernportal zur Vertiefung der Kenntnisse der Mitarbeiter

- **Social Engineering Angriff 3: Schadcode-E-Mail**
  - E-Mail mit Attachment oder Download-Link einer Schadcode-Datei in einer Word-Datei
  - Anwender wird zum Öffnen der Datei und Ausführen von Makros aufgefordert
  - Schadcode meldet zurück, welche User die Datei geöffnet haben

Idealerweise führt ein erfolgreicher Angriff zu einer Weiterleitung des Mitarbeiters direkt auf das Lernportal zur Vertiefung der Kenntnisse.




### Baustein 5: Lernportal

Abhängig von den Ergebnissen des Social Engineering Tests kann für einzelne Benutzergruppen eine Nachschulung notwendig werden. Diese Nachschulung kann wieder als Live Awareness Seminar mit Referenten oder über das Lernportal mit Abschlusstest und Nachweis durchgeführt werden.

### Baustein 6: Neue Awareness Kampagne

Die initiale Awareness Kampagne wird mit aktualisierten Inhalten und Themen sowie neuer grafischer Darstellung wiederholt. Dadurch soll die Erinnerung der Mitarbeiter aufgefrischt werden. Möglich ist wieder eine Kampagne mit Postern an sichtbaren und erkennbaren Stellen im Unternehmen aber auch alternative Mittel wie z.B. Mauspads etc. mit Informations-sicherheits-Tipps.

### Baustein 7: Aufrechterhaltung der Awareness

Die Aufrechterhaltung der Awareness erfolgt am besten durch regelmäßige Nach-schulung.

Denkbar ist hier aus Kostengründen ein Wechsel zwischen Awareness Seminaren im ersten Jahr sowie einem Online Lernportal mit Videos im zweiten und dritten Jahr, bevor im vierten Jahr wieder mit Live Awareness Seminaren neu begonnen wird.

**NESEC**
**Gesellschaft für angewandte Netzwerksicherheit mbH**

Fürholzener Straße 5a
85386 Eching
Telefon: 089 - 45217100
E-Mail: welcome@nesec.de
Internet: www.nesec.de

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH