FIS-ASP Application Service Providing
und IT-Outsourcing GmbH
Röthleiner Weg 4, D-97506 Grafenrheinfeld

FACTSHEET

WIE SECURITY AWARENESS TRAINING IHR BUSINESS SCHÜTZEN KANN

SECURITY AWARENESS

Ziel des Security Awareness Trainings ist es, Mitarbeitende mit dem Know-how zum Erkennen und zur Abwehr der Bedrohungen auszustatten, indem sie Hauptmerkmale von Cyberangriffen und Mittel für eine effektive und nachhaltige Abwehr kennenlernen.

INHALT

Warum sind Security Awareness Trainings so wichtig?

Cyberkriminelle werden auch zukünftig weiterhin auf Phishing-Attacken zurückgreifen, da die bereits vorhandene, technische Sicherheit vieler Systeme deren Angriffsmöglichkeiten reduziert und infolgedessen der Mensch inzwischen als letztes Glied in der Kette in den Fokus gerückt ist und sich als überaus lohnender Angriffsvektor präsentiert.

Unabhängig von der Unternehmensgröße reicht **ein** abgelenkter bzw. unvorsichtiger Angestellter aus, um folgenschwere Auswirkungen für das Unternehmen auszulösen.

Jedem fünften

Unternehmen wurden schon Daten & Informationen gestohlen, als Folge von Mitarbeitermanipulationen. Cyber-Kriminelle nutzen gerade das Arbeiten im Homeoffice für sich aus.

SENSIBILISIERUNGSMAßNAHMEN

Wiederholende und gut aufeinander aufgebaute Sensibilisierungsmaßnahmen bei Ihren Angestellten sind der passende Schlüssel, um Phishing-Angreifern den Wind aus den Segeln zu nehmen und das Sicherheitsrisiko Ihres Unternehmens kontinuierlich zu senken.

WELCHE SCHULUNGSINHALTE SIND HIERFÜR GEEIGNET?

Damit sich Sicherheitsschulungen für Ihr Unternehmen lohnen, sind trockene Lerninhalte, die nicht zur Risikominderung beitragen, ungeeignet. Sie benötigen Kurse, die den Endbenutzer darauf vorbereiten Bedrohungen zu erkennen und richtig darauf zu reagieren.

Dabei sollten die Trainingseinheiten auf Ihrer Branche und Ihrem Unternehmen zugeschnitten sein. Außerdem eignen sich simulierte Angriffe im Arbeitsalltag als ein wichtiger Teil der aktuellen Risikobestimmung (*„Wie viele Mitarbeitende klicken auf die simulierte Ransomware Mail?“)* und als Lernprozess, um alle Mitarbeitenden über die zunehmende Gefahr von Hacking und Social-Engineering-Angriffen auf dem Laufenden zu halten und zu sensibilisieren.

LASSEN SIE IHRE ANGESTELLTEN GESCHÜTZT FÜHLEN

Betrachten Sie Ihre Belegschaft nicht als schwaches Glied, sondern geben Sie Ihren Mitarbeitenden das Vertrauen in ihre Fähigkeit, Cyber-Bedrohungen zu erkennen. Ein wichtiger Teil effektiver Schulungen ist es, Hand in Hand mit Ihren Mitarbeitenden zu arbeiten. Der Lehrplan sollte motivieren, Ihr Unternehmen sicher zu halten und auf Phishing-Attacken zu achten.

Es sollte ein offener Raum für Diskussionen, Zusammenarbeit und Verbesserungen geschaffen werden. Dabei sollten alle Abteilungen gleichermaßen in Schulungen und in den Informationsaustausch einbezogen werden – ohne, dass der Prozess als langwierig oder langweilig empfunden wird.

Außerdem sollten Ihre Mitarbeitenden sich darin bestärkt fühlen, ihre Fähigkeiten zu erweitern, indem der individuelle Kenntnisstand und die daraus abgeleiteten Schulungsbedürfnisse berücksichtigt werden.

STÄRKEN SIE IHRE HUMAN FIREWALL

Als ein kompetenter Partner stehen wir Ihnen zur Seite und unterstützen Sie auf Ihrem Weg zur Aktivierung Ihrer Human Firewall mit unter anderen folgenden Maßnahmen:

- ✓ *Einrichten einer Awareness- und Pishing-Test-Plattform*
- ✓ *Unterstützung bei der Implementierung und Ersteinrichtung der Plattform mit regelmäßig stattfindenden Abstimmungen*
- ✓ *Ausarbeitung von verschiedenen Kampagnen in Zusammenarbeit mit Ihnen und unseren IT-Security ExpertInnen*
- ✓ *Erstellen oder Beratung bei simulierten Phishing-Mails - zugeschnitten auf den Arbeitsalltag Ihrer Mitarbeitenden*
- ✓ *Durchführung von Analysen und Auswertungen der Ergebnisse*

Schärfen Sie das Sicherheitsbewusstsein Ihrer Organisation und wehren Sie Cyberattacken mit der Kombination aus Fachwissen und dem richtigen Verhalten Ihrer Mitarbeitenden ab.

FIS-ASP Application Service Providing
und IT-Outsourcing GmbH
Röthleiner Weg 4
D-97506 Grafenrheinfeld
www.fis-asp.de