

Unser IT-Security-Awareness-Programm

IT-Security Awareness

Aktuellen Studien¹ zum Thema Cyberkriminalität, Datendiebstahl und deren Methoden zeigen, **dass 66% aller Malwareinfektionen über Mails geschehen und 81% aller erfolgreichen Angriffe über gestohlene oder zu schwache Passworte erfolgen.**

Diese Angriffsflächen sind technisch nur schwer zu beseitigen. Hier obliegt es dem Endnutzer und aufmerksamen Mitarbeiter verdächtige Mails oder Phishing-Versuche zu erkennen.

Grundsätzlich sind diverse Social-Engineering Methoden bekannt mit denen Cyberkriminelle, Mitarbeiter überlisten, um Zugang zu sensiblen Daten und Systemen zu erhalten. Unser Awareness-Programm fokussiert sich hierbei auf das Assessment und die Sensibilisierung Ihrer Mitarbeiter gegen:

- **Phishing-Kampagnen** (Userdaten- & Passwortabgriff)
- **Malware Delivery via Mail**
- **Drive-by Malware Deployments** über böartige Websites

Hierzu bieten wir neben **zwei Assessmentpaketen** auch einen **Self-Service E-Learning-Kurs** zur Sensibilisierung an.

Unsere Assessments werden speziell für Ihr Unternehmen zusammengestellt und umfassen:

- Konzeption/Storybuilding einer individuellen Phishing- oder Malware-Delivery-Kampagne.
- Bereitstellung der technischen Plattformen für Assessment und E-Learning.
- Detaillierte Berichterstellung über den Erfolg des Assessments.
- Auf Wunsch Einbindung eines E-Learning-Programmes zur Sensibilisierung der Mitarbeiter.

Mit unserem **Security-Awareness - Programm** ist es Ihnen möglich:

- Über realistische Assessments Ihre Mitarbeiter für Social-Engineering-Gefahren zu sensibilisieren.
- Die Gefährdung Ihres Unternehmens gegenüber dem aktuell bedeutendsten Cyberangriffsvektor zu beurteilen.
- Auf Basis der Ergebnisse weitere Schritte zur Minimierung der Gefahren durch Social Engineering einzuleiten.

¹Siehe: Verizon Data Breach Investigations Report (DBIR) 2017

