CyberSecurity

AIRBUS

# Social Engineering Penetration Tests

## Wir schlüpfen für Sie in die Rolle von Cyber Angreifern und testen den Status Quo Ihrer IT-/OT-Sicherheitskultur

„Trickbetrüger ergaunern Passwort vom CEO“

– solche Schlagzeilen lesen wir heutzutage fast täglich. Wir können uns allerdings nicht vorstellen, dass Sie Ihren Unternehmensnamen in derartigen Artikeln lesen wollen. Damit Sie die Methoden der Cyber Angreifer vorzeitig entlarven, bieten wir Social Engineering Penetration Tests an.

Ein Social Engineering Penetration Test ist **eine geplante und zielgerichtete Attacke, die Ihre Mitarbeiter auf ihr Informationssicherheitsverhalten hin prüft**. Sie zeigt Ihnen auf, in welchem Maße Informationssicherheit in Ihrem Hause gelebt wird und wie wirksam Ihre bereits durchgeführten Awareness-Maßnahmen sind. Ferner gibt sie Ihnen die Chance, Ihre zukünftigen Maßnahmen besser planen zu können.

**Das machen wir an drei Punkten fest:**

- Sie erhalten **mehr Transparenz über die möglichen Risiken**, die von einer Social Engineering Attacke ausgehen,
- Sie überprüfen die **Einhaltung Ihrer Informationssicherheitsrichtlinien** und
- Sie verbessern die **Awareness gegenüber diesen Attacken bei Ihnen und Ihren Mitarbeitern**.

**Durch die höhere Transparenz der Risiken ist es für Sie leichter, ein besseres Risikomanagement zu betreiben.** Daraus wiederum resultiert, dass Sie bessere technische, organisatorische, personelle und infrastrukturelle Maßnahmen gegen solche Attacken ergreifen können, was wiederum zu einer Reduzierung der Wahrscheinlichkeit eines erfolgreichen Angriffs führt.

Nebenbei bekommen Sie Informationen darüber, welche **Nachbesserungen in Ihren Informationssicherheitsrichtlinien durchgeführt werden müssen** und Sie erkennen, welche Akzeptanz und welchen Stellenwert die Informationssicherheit bei Ihren Mitarbeitern hat. Natürlich bekommen Sie auch **Einblick in die neusten Methoden der Angreifer** und wie trickreich sie versuchen, an Wissen in Ihrem Unternehmen zu gelangen.

Im Rahmen der kundenspezifischen Vorbereitung und Planung der Social Engineering Attacke werden u.a. Social Media Plattformen oder Firmenvideos und Broschüren nach Hinweisen untersucht, die möglichen Angreifern helfen können, in Ihr Unternehmen einzudringen.

# Social Engineering Penetration Tests

**Wir schlüpfen für Sie in die Rolle von Cyber Angreifern und testen den Status Quo Ihrer IT-/OT-Sicherheitskultur**

**Die Bausteine, aus denen unser Service besteht sind:**

| | |
|---|---|
| **Media Dropping**  | Im Gebäude sowie an öffentlich zugänglichen Plätzen (Großraumbüro, Besprechungsräume, Produktionshalle, Bistro, etc.) werden präparierte USB-Sticks platziert, die später von Mitarbeitern ggf. eingesteckt werden. |
| **(Spear) Phishing**  | Mit Hilfe von präparierten E-Mails, die den Eindruck von Seriosität vermitteln, wird untersucht, ob und wie viele Mitarbeiter den in der E-Mail enthaltenen Link anklicken. |
| **Tailgating**  | Es wird versucht, physische Sicherheitsbarrieren auf ihre Funktion hin zu überprüfen und zu überwinden. Im Anschluss wird untersucht, in wie weit reale Angreifer sich innerhalb Ihrer Organisation physisch fortbewegen könnten. |
| **Pretexting**  | Über gezielte Telefonanrufe wird versucht, sensible Informationen über Ihre Organisation, ein Projekt oder sonstige interne Angelegenheiten in Erfahrung zu bringen. |
| **Report**  | Der Report beschreibt die durchgeführten Methoden im Detail und stellt die Ergebnisse übersichtlich dar. Darüber hinaus werden die Ergebnisse hinsichtlich der daraus resultierenden Risiken betrachtet und individuelle Verbesserungspotenziale vorgestellt. |

Wichtig ist, dass es in unseren Social Engineering Penetration Tests nicht darum geht Fingerpointing zu betreiben oder Mitarbeiter bloßzustellen. Es geht einzig und allein darum, zu testen, ob bisherige Informationssicherheitsmaßnahmen auch gelebt werden und das Wissen und die Wahrnehmung über mögliche Angriffsvektoren zu erhöhen.

Dabei versteht es sich von selbst, dass wir alle Informationen streng vertraulich behandeln.

Sprechen Sie uns für ein spezifisches Angebot für Ihr Unternehmen an.

AIRBUS



**Airbus CyberSecurity**
**Frankreich**
Metapole 1, boulevard Jean Moulin
CS 40001
78996 Elancourt Cedex

**Deutschland**
Willy-Messerschmitt-Str. 1
82024 Taufkirchen

**Vereinigtes Königreich**
Quadrant House
Celtic Springs - Coedkernew
South Wales NP10 8FZ

**Vereinigte Arabische Emirate**
Etihad Towers T3
Corniche Road, 19th floor
P.O.Box: 72186
Abu Dhabi

**contact.cybersecurity@airbus.com**
**www.airbus-cyber-security.com**