

Social Engineering Penetration Tests

We take on the role of cyber attackers and test your IT/OT security culture

“Cyber-attacker steals password from CEO” - we read these types of headlines almost daily these days. However, no one would want to see their company’s name in such articles. We offer Social Engineering Penetration Tests to expose the methods of cyber criminals before they can attack.

A Social Engineering Penetration Test is a **planned and targeted attack that tests the information security behaviour of your employees**. It shows you how much information security you have internally and how effective the measures you take to increase awareness are. This will also give you the chance to better plan your future activities.

For this, **we provide you with three fundamental insights**:

- **Increased transparency** regarding the potential risks of a social engineering attack
- **Compliance testing** with your information security policies
- **Heightened awareness** for you and your employees regarding these types of attacks

Greater transparency in regards to risks will improve your risk management. This in turn means that you can take better technical, organisational, human and infrastructural measures to reduce the likelihood of a successful attack.

You will also be informed of the **improvements that need to be made to your information security guidelines**, and you will be able to recognise how much your employees value information security and to what extent they accept it. Of course, you will also learn about the **latest methods used by attackers** and the clever methods they use to try to gain knowledge about your business.

As part of the customer-specific preparation and planning of the social engineering attack, resources such as social media platforms or company videos and brochures will be examined for clues that could help potential attackers infiltrate your business.

Social Engineering Penetration Tests

We take on the role of cyber attackers and test your IT/OT security culture

Our service consists of the following building blocks

Media Dropping



Prepared USB sticks, which may later be plugged in by employees, are placed in the building as well as in publicly accessible places (open-plan office, meeting rooms, bistro, etc.).

(Spear) Phishing



Prepared e-mails that appear credible will be sent to see whether employees click on the link within and if so, how many.

Tailgating



We will check that the physical security barriers in place are working and attempt to get around them. We will then examine how far real attackers could physically move within your organisation.

Pretexting



Targeted phone calls will be made to attempt to gather sensitive information about your organisation, a project, or other internal matters.

Report



The report will describe the methods used in detail and clearly display the results. The results will be examined with regard to the resulting risks and potential individual improvements will be presented.

Please note that our Social Engineering Penetration Testing is not about finger-pointing or singling out employees. The goal is to see whether previous information security measures are in place and to raise understanding and awareness of potential angles of attack.

It goes without saying that we treat all information as strictly confidential.

Contact us for more information.

AIRBUS

This document is not contractual. Subject to change without notice. © 2019 Airbus CyberSecurity. AIRBUS, its logo and the product names are registered trademarks. All rights reserved. // 917 E 0875

Airbus CyberSecurity

France
Metropole 1, boulevard Jean Moulin
CS 40001
78996 Elancourt Cedex

Germany
Willy-Messerschmitt-Str. 1
82024 Taufkirchen

United Kingdom
Quadrant House
Celtic Springs - Coedkernew
South Wales NP10 8FZ

United Arab Emirates
Etihad Towers T3
Corniche Road, 19th floor
P.O.Box: 72186
Abu Dhabi

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

