# Penetration testing using social engineering practices

AEC

## We can help you create awareness and reduce the risk of penetration

Due to a lack of awareness, the human factor is the number one security risk to data and information for all companies. Educating users significantly reduces the risk of data leaks

During the social engineering tests, we will tailor the training plan to your needs. We will carry out a test involving information gathering, vishing, spear-phishing or physical intrusion. We present the results in a report that identifies your users' level of awareness and your organization's vulnerabilities. We present the specific measures you should take that are specially adapted to increase your protection against threats - whether internal or external.

aec-security.eu

## Penetration testing using social engineering practices

**Phishing as a service** - we carry out email penetration testing either on a one-off basis or as a continuous campaign. The aim of the phishing campaign is to check the current state of the company's security and employee awareness via a simulated phishing attack.

**Vishing as a service** – this is penetration testing over the phone, which, as with phishing, is either in a one-off or an ongoing form. The test itself is a simulation of a real telephone attack. During a fraudulent phone call, the attacker tries to gain information or persuade the user to do something that could compromise your organization's security.

**Penetration testing using social engineering practices** – this is a comprehensive service that can involve a combination of phishing, vishing and physical infiltration. Here our team of social engineers try to infiltrate an organization's protected areas. The service helps detect susceptibility to attacks that use social engineering practices.

**KnowBe4** – this is the world's largest integrated platform for training employees in security. It offers simulated phishing or vishing attacks or ascertains employees' reactions to unknown USB devices. Apart from the ability to simulate attacks, the platform also offers training videos on phishing, security awareness, passwords, email security, malware and more.

# Penetration testing using social engineering practices

AEC

## Phishing

This is one of the best-known attacks using social engineering and simply involves sending out potentially malicious emails that look as though they come from trusted sources. The targets of phishing can be divided up as follows:

- delivering malicious data that provides remote attackers with access
- collecting login data
- collecting further snippets of information for further attacks

The phishing service aims to educate employees by simulating an attack. We send out an email that detects user behaviour as soon as it is delivered. This gives us statistics that show to what extent employees are susceptible to the phishing attack vector and where further training will be needed. Two reports are then compiled, the first is an interim one that gives information on the actions the users took and also includes all the metrics measured. The second, a more formal one, includes a description of the scenario, the data obtained, a description of user behaviour, recommendations and comparisons with previous campaigns.

## Vishing

This can be defined as telephone phishing. During a fake phone call, the attacker uses social engineering methods to get the victim to share information and take a specific action.

- Share certain information
- Carry out a specific action

Vishing as a service also has an educational component. It involves a number of phone calls made by humans. The service has a team of social engineers who use dynamic guises to continuously gather critical data from employees. During the internal penetration test, we use VoiP technology to replace caller ID with a trusted source, for the external test, calls come from phone numbers outside the organization. We tailor call scenarios to suit your company and record individual calls for educational purposes. The output is a formal report with a detailed description of the scenarios, the metrics measured, user actions, comparisons to previous campaigns and recommendations.

## Penetration testing from the social engineering standpoint

During this comprehensive test we use phishing, vishing and physical infiltration. At the start of the test, the company identifies its critical assets. Our team of social engineers then researches the information across the Internet and the darknet, always focusing on the company's critical assets. Based on the information gathered, we develop potential attack scenarios. Then there is the actual penetration test, which verifies the existing process or policy in place in relation to the defined assets. The output is a detailed report describing the scenarios, user behaviour and recommendations.

## KnowBe4

This platform provides a user-friendly environment that allows you to simulate phishing attacks. It includes thousands of templates with unlimited use as well as the largest library of security awareness training, including interactive modules, videos, games, posters and newsletters. KnowBe4 allows you to hold automated training campaigns with scheduled email reminders. The resulting reports are then created from phishing tests and training sessions.

More on a specialized website .....
**www.socialing.cz**

## Our advantages

- We are a successfully established Czech security company that has been on the market for over 30 years.
- We have more than a decade of experience in social engineering.
- Our team is made up of specialists with experience from hundreds of sub-projects
- We hold eMAPT, CISSP, OSCP, OSCE, CEH and many other certifications.
- We run our own hacking lab to research numerous areas dealing with security in various solutions
- We listen to our clients and adapt our tests to their needs and time constraints
- We follow the latest trends in social engineering.
- We focus on the organization's specific needs during the tests

**Prague** – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
**Brno** – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
**Bratislava** – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283