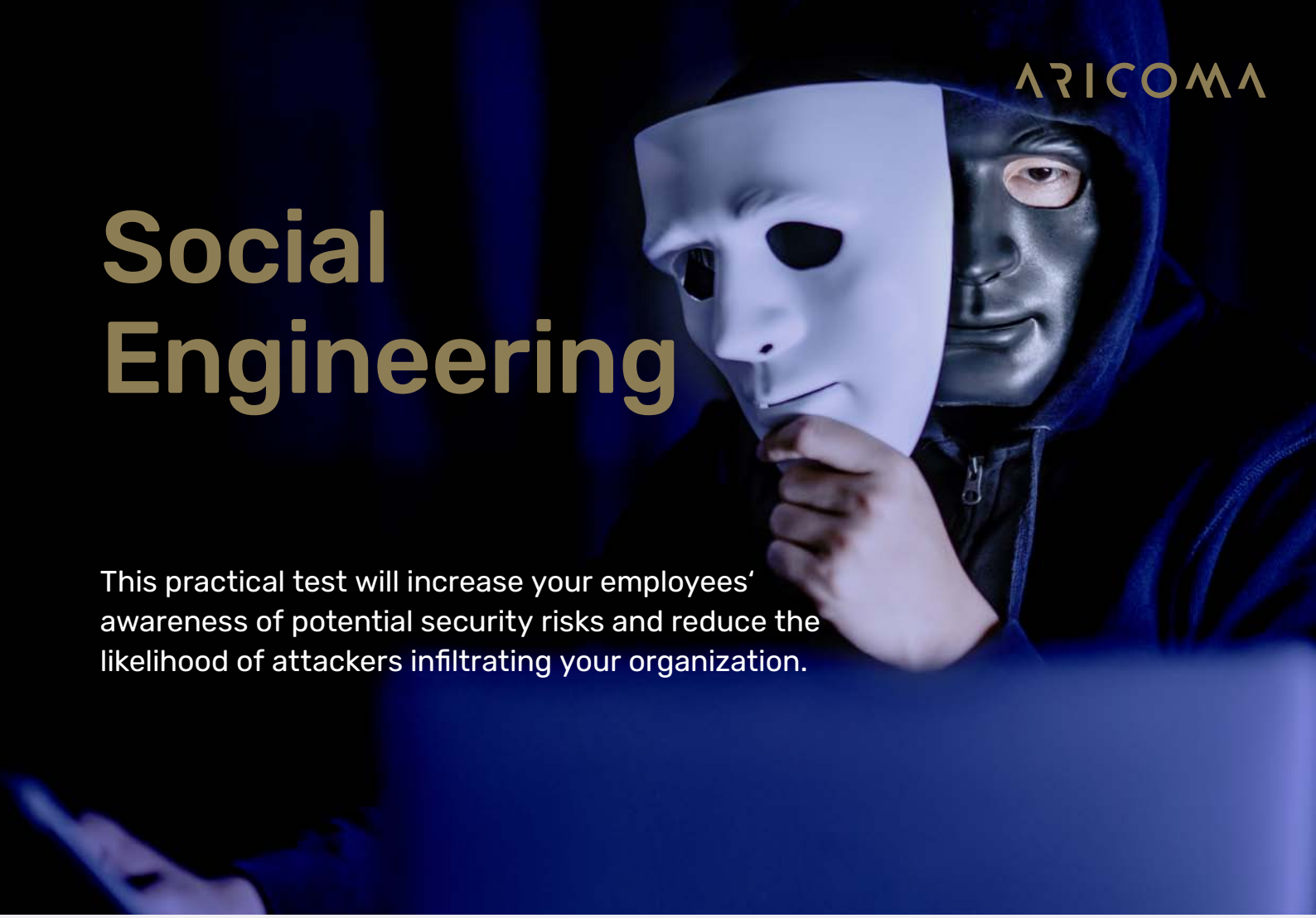

Social Engineering

This practical test will increase your employees' awareness of potential security risks and reduce the likelihood of attackers infiltrating your organization.

Penetration tests using social engineering

Phishing as a service

We perform email penetration tests on a one-off basis or as a continuous campaign. The aim of the phishing campaign is to test the current state of the company's security and employee awareness using a simulated phishing attack.

Vishing as a service

This involves telephone penetration tests, which, like phishing, are conducted as a one-off test or continuous penetration test using social engineering.

The test itself is a simulation of a real telephone attack. In a fraudulent call, the attacker tries to obtain information or persuade the user to take action that could compromise your organization's security.

KnowBe4

KnowBe4 is the world's largest integrated platform for employee security training. It **offers simulated phishing and vishing attacks**, or determines how employees react to an unknown USB device.

In addition to attack simulations, the platform also offers educational videos on phishing, security awareness, passwords, email security, malware and more.

Penetration test using social engineering

A service that can involve a combination of phishing, vishing and physical infiltration, in which our team of social engineers attempt to penetrate an organization's protected premises. **The service helps to detect vulnerabilities exploitable through social engineering attacks**.

Phishing

Phishing is one of the most well-known social engineering attacks and involves sending out potentially malicious emails pretending to come from trusted sources.

Phishing targets are divided into:

- delivery of malicious data that provides access to remote attackers,
- collection of login data,
- gathering additional information for further attacks.

The goal of phishing as a service is to educate employees by simulating an attack. We send out an email that detects user behavior as soon as it is delivered. The result is statistics that show the extent to which employees are susceptible to the attack vector and where further training will be needed.

The output is two reports - interim and formal. The interim report describes on actions taken by users and also includes all measured metrics. The formal report includes a description of the scenario, data collected, user behaviour, recommendations and comparison with previous campaigns.

Vishing

Vishing is like phishing over the phone. These are calls with a fully human-driven approach. The service is performed by a team of social engineers, where we use dynamic excuses to continuously gather critical data from employees.

During the internal penetration test, we use VoIP technology to replace caller ID with a trusted source, while in the external test, calls come from phone numbers outside the organization.

We prepare customized call scenarios and record individual calls for educational purposes. The output is a formal report that includes a detailed description of the scenarios, the metrics measured, actions taken by users, comparisons with previous campaigns, and recommendations.

KnowBe4

KnowBe4 provides a user-friendly environment that allows you to perform simulated phishing attacks. It includes thousands of unlimited-use templates as well as the largest cybersecurity training library, including interactive modules, videos, games, posters and newsletters.

KnowBe4 allows you to run automated training campaigns with scheduled reminder emails. The resulting reports are then made up of phishing tests and training.

Benefits

- We will check the security awareness of your organization's members.
- We'll identify any weak points and report them to you.
- Completing the test will reduce the likelihood of your data being leaked.
- We have more than 10 years' experience in social engineering.
- Our team consists of specialists with experience from hundreds of sub-projects.
- We hold eMAPT, CISSP, OSCP, OSCE, CEH and many other certifications.

For more information, visit www.socialing.cz

Penetration test from a social engineering perspective

In this comprehensive test we use phishing, vishing and physical infiltration. At the beginning of the test, you will identify your critical assets. Our team of social engineers then performs a survey of information across the internet and darknet, focusing on the critical assets thus identified.

Based on the information gathered, we will develop potential attack scenarios. We will then perform a penetration test to validate the existing process or policy against the defined assets. You will subsequently receive a detailed report describing the scenarios, user behavior and recommendations.