SOCIAL ENGINEERING

Human behaviour is one of the weakest links in an organization's computer security, hence the necessity to periodically test such behaviour. Social engineering allows for the psychological manipulation of people to perform unwanted actions.

The service includes multiple types of phishing attacks via phone calls, text messages, and emails that are designed to convince an employee to disclose sensitive information or to perform malicious/inadvertent actions (e.g. disclosing their password, running a malicious code, opening an "entrance gate" to the company, etc.). For the tests, we use our internally-developed framework and methodology that simulates a real attack.

SERVICE OVERVIEW

The purpose of social engineering tests is to verify employee security awareness. The test results in a report that contains a detailed analysis of the conducted tests with an executive summary.

The cost of the social engineering test depends on the depth and complexity of the test, and the size of the tested company. The price is determined after customer consultation, which determines the scope, type of test, and other requirements from the customer.

The test can be performed using the BLACK BOX (no information about the tested company), GREY BOX (partial information about the company) or WHITE BOX (all necessary information about the company) method. Depending on the agreed method, the first phase of the test will be adapted accordingly. The first phase deals with the collection of information about the company being tested (information on employees from publicly available sources / social networks, used IT assets, etc.).

We offer several types of tests that vary in the scope and depth of the test. After discussing with the customer, we recommend the type and scope of the appropriate company-specific test.

PHISHING TEST

- Phishing test - phishing campaign targeted at all company employees
- Spear phishing test - phishing test targeted at a narrow group of people in the company

A phishing / spear phishing email attempts to force the people being tested to make an unwanted action (password change, visiting a website with malicious code (drive-by attack), visiting a fake site, downloading an attachment, and executing a malicious code (RAT, ransomware, keylogger, etc.)).

VISHING/SMS PHISHING

Unlike classic phishing, this type of phishing is performed via phone call or text message. This type of attack also aims to attempt to obtain confidential, commercial data, or make an unwanted action (password change, etc.). If possible, the caller/sender ID is fake (spoofed).

PHYSICAL/ON-SITE (BAITING)

A physical version of a social engineering test, where portable media (CDs, DVDs, USB keys) are left around the premises of the tested company. The media contain a malicious code (RAT, ransomware, keylogger, etc.) or only an executable code that serves the final evaluation of the test.