IstroSec

Data Sheet

Attack Simulations

IstroSec offers the opportunity to test the effectiveness and efficiency of security measures through simulated attacks. In this way, it is possible to verify that employees are sufficiently aware of and can withstand cyber threats, and that your preventive, detective, and reactive measures work as intended. We offer simulations of attacks by social engineering and simulations of an attacker present in your infrastructure.

> *During an attack simulation, you can verify that both the incident response team and the management can respond to incidents quickly and efficiently.*

Social engineering simulations:

- Phishing
- Vishing
- Spearphishing
- Smishing
- Whaling
- Physical Social Engineering

Social Engineering Attack Simulations

Comprehensive resistance to attacks by social engineering can be achieved by an advanced training program of employees, adequate technical measures, and regular testing of their effectiveness. IstroSec is ready to help you increase your readiness and resistance to these types of attacks.

Phishing Simulations

Our experts will prepare and implement a phishing campaign that will not be targeted at specific employees, or the technologies or services used. As part of this campaign, a list of employees' email addresses will be compiled based on publicly available data. Subsequently, a phishing email will be sent to these addresses in an attempt to solicit login information, personal information or other sensitive information, or download the attachment.

Spearphishing Simulations

Spearphishing is a more advanced and more effective type of phishing. In this simulation, our experts use open-source intelligence (OSINT) to obtain the data needed to prepare a targeted and highly effective campaign that will take into account the specifics of your technologies, employees or services used. Very similar domains, bypassing multifactor authentication or deploying specific malware written by our malware analysts are used.

Whaling

As part of the whaling attack simulations, our experts will carry out a spearphishing campaign aimed at the top management of the organization. It is the attack on this group of people that can cause significant damage to an organization by combining their access to critical information and dynamic work styles.

Vishing

Voice phishing attacks can be a very effective way to solicit sensitive information from employees. Our experts will carry out a telephone attack using information from OSINT and employ psychological manipulation, impersonation, and fraudulent tricks.

Smishing

We will send phishing SMS messages to your employees to solicit login details, personal data or other sensitive information or download an email attachment.

Physical social engineering

Our experts will visit your workplace and, through communication with employees, will seek information that can be used to conduct other attacks, install malicious software, obtain passwords, sensitive data, or force employees to perform activities that violate the organization's security policies.

Simulations of an attacker already present in your infrastructure

Simulations of specific activities of the attacker

Simulations of an attacker's specific activities in an organization can consist of activities such as lateral movement, the spread of malicious code, data collection and filtering, circumvention of security measures in the organization, and other activities.

Simulation of a complex attack against an organization

During this type of simulation, we test your security team's detection and response capabilities for the tactics, techniques, and procedures (TTPs) of advanced persistent threats (APT). If a particular APT group is currently focusing on your business sector, we can help you increase your ability to withstand its specific TTPs. For example, in the case of the APT41 group, it could be spearphishing with a malicious attachment, WMI, scheduled tasks, PowerShell, DLL Side-Loading, SMB / Windows Admin Shares, keylogging, or data encryption as an exit strategy.

Why IstroSec?

In addition to high skills in performing the simulations themselves, **Istro**Sec experts thoroughly study the tactics, techniques and procedures used by attackers in the wild. Thanks to this combination, the client can safely test their resilience and readiness for real attacks.

Case Study

Company type: financial institution
Service provided: spearphishing simulation
Solution: Spearphishing test and malware creation

The organization was interested in verifying the configuration of already existing email solution protections, as well as the behavior of all employees when they receive unsolicited e-mail in the company's e-mail box. It was possible to test such a case by using **Istro**Sec services such as phishing simulation or, as in this case, a targeted and more effective spearphishing campaign.

In the initial (reconnaissance) phase, this included obtaining information about the company and employees. Thanks to this, we were able to obtain employees' email addresses, information about the mail infrastructure, the protections used and more. Subsequently, a campaign was prepared which may, for example, include a link to a website simulating the original website to obtain access data and the second authentication factor. Alternatively, we can create malware for the needs of a sophisticated campaign that can simulate ransomware or other forms of behavior of a real attacker.

During the creation of the payload, a final email is proposed, which will then be sent to a selected group of employees at a predefined time. After the campaign is sent out, the results are analyzed, and after the end, the final report is handed over to the customer. The report contains an executive summary, identified weaknesses, detailed statistics such as the number of emails sent, link clicks, data sent, list of devices from which the phishing site was accessed and more.