Sonpo

PENETRATION TESTING SERVICES

The National Cyber and Information Security Agency (NÚKIB) defines penetration testing and vulnerability testing as one of the obligations arising from Decree **No. 82/2018 Coll., on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal.**

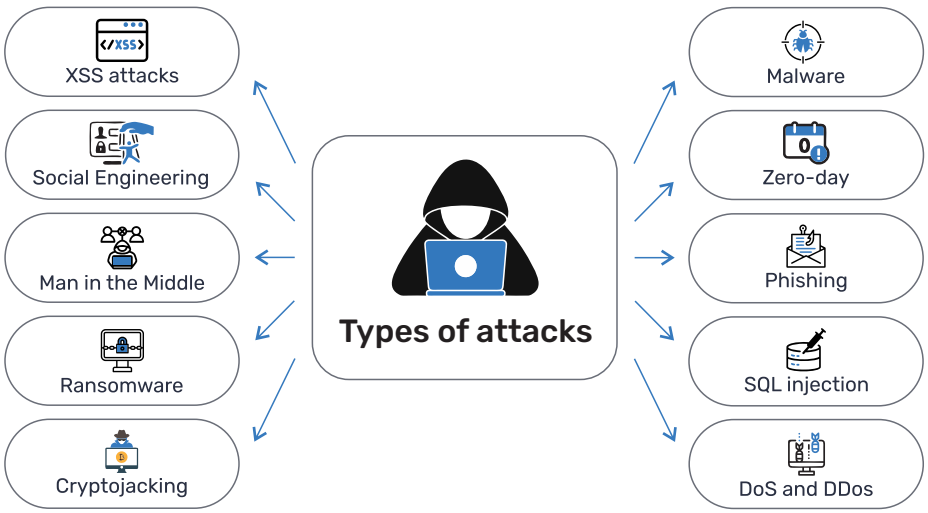
OFFER OF TESTS

EXTERNAL PENETRATION TESTS:

- **Web application tests**
- **Mobile app tests**
- **Information gathering** *(OSINT)*
- **Perimeter tests** *(firewall, DMZ, DNS, ...)*
- **E-mail system tests** *(DMARC, ...)*
- **Phishing tests** *(spear phishing)*

INTERNAL PENETRATION TESTS:

- **Infrastructure tests** *(VLANs, WiFi, virtualisation, ...)*
- **Station and Active Directory tests** *(configuration, passwords, ransomware, ...)*
- **Server tests and audits** *(Linux and Microsoft)*
- **Tests and audits of e-mail servers** *(cloud, local, sandboxing, ...)*



TYPES OF TESTS

Black-box tests

Black-box tests simulate an external access of an attacker who only knows general information but not the internal structure of an application, server or network. The functionality of the system itself is a black-box for the tester.

White-box tests

Compared to the previous type of tests (black-box), these tests are typically input knowledge-based. This kind of testing requires documentation about the applications, servers or networks being tested.

Grey-box tests

This is a combination of the above-mentioned tests. The tester is given only partial knowledge of the tested system and then proceeds as in black-box testing.

Sonpo

RECOMMENDED POST-TESTING PROCEDURES

- Based on the evaluation of the results of the penetration testing, the identified deficiencies **should be corrected without delay**.
- After the first penetration testing, a large number of **real exploitable security vulnerabilities** are usually revealed. If the identified vulnerabilities are consistently corrected, each subsequent penetration test should reveal fewer real exploitable vulnerabilities, but the effect on the practical security of the entire system is all the greater.
- If an organisation does not **adequately respond** to the results of penetration testing, or does not implement the removal of the identified deficiencies, then the actual performance of penetration testing will not have any added value for the system administrator.

VULNERABILITY ASSESSMENT BY SEVERITY LEVEL

CRITICAL	HIGH	MEDIUM	LOW
Exposed vulnerabilities can be immediately exploited to completely compromise the system.	Discovered vulnerabilities which in combination with other vulnerabilities or practices ("social engineering") pose a high risk.	The special conditions for exploiting these vulnerabilities must be met or their potential exploitation has a limited impact.	Minor security issues.

OUTPUTS FROM PENETRATION TESTS

- The output of Penetration Tests is a **final report** – a document describing the state of the given IS areas from the security point of view with a proposal of recommendations. The resulting report contains, for each IP address/server tested, the date and time of testing, the OS version detected, and a list of vulnerabilities with different **severity levels**.

- The report also includes management summaries and test results for individual applications, services or systems. The results contain a list of discovered **vulnerabilities** ranked by severity – critical, high, medium or low. Each revealed vulnerability is accompanied by a **detailed description, severity level** and **recommendations** on how to fix the vulnerability.

- The contractor shall ensure to the maximum extent possible that testing is **non-destructive** and **does not cause system crashes, modification or deletion of data**. This does not apply to data modification, such as logs, which are caused by normal system usage (for example, an increase in access logs).

- The testing procedure is based on **OSSTMM, OWASP, PTES** and **NIST 800-115** methodologies and recommendations of the National Cyber and Information Security Agency (**NÚKIB**).

CUSTOMER INTERACTION

For a successful implementation within the given deadlines and proper provision of support services, it is necessary to provide cooperation from the customer, in particular to:

- Specify **applications and relevant servers** for testing purposes (IP addresses, server names).
- Specify and provide an appropriate **time frame** for testing.
- Define **IP addresses** of devices which have specific requirements for test execution (execution time, or other restrictions).
- Create a **suitable virtual environment** on the customer's internal network from which automated testing tools will be run.
- Fulfil the **general principles** of the project management and to create conditions for the fulfilment of obligations arising from the implemented agreements so as to avoid delays in the fulfilment of individual deadlines for the provision of performance.
- During each activity, interested **customer representatives** will be available by prior arrangement, i.e. to provide contact information (cell phones and emails to customer administrators).
- Provide customer **management support** for the duration of the project.
- Ensure the provision of **complete, truthful and timely information** that is or may be required for the proper performance of the contractor's obligations.
- Ensure the **provision of all information**, documents, internal documents, legal standards, regulations, directives, instructions and methodological regulations related to or affecting IT operations management and security. Delivery of these materials shall be arranged by the customer's Authorised Person within 2 days of the signing of the Contract/Order or within 2 days of an official request from SONPO.
- Participate in **scheduled meetings**, teleconferences and handle assigned tasks in an orderly and timely manner.

SONPO, a.s. | Prague | Czech Republic
www.sonpo.eu | sales@sonpo.eu