SOFLAB

IT security
Security audits and penetration tests

Will you **benefit from our service?**

- **You need to protect data** and maintain business continuity.
- **You want to implement security tools** but you lack the resources.
- **You need personalized reports** to fulfill conformity requirements and legal regulations.
- **You have a technical support team**, but you need to know more about security.
- **You want to make sure,** your internal infrastructure is secure and there is no possibility of divulging the secrets of your business through unauthorized actions performed by employees or partners working inside the network.

Through a combination of expertise and technological know-how, Soflab Technology helps organizations optimize the security and quality all throughout the software's life cycle.

106 days
it takes this much time for companies in Europe to detect a cyberattack

56%
of organizations can't detect complex cyberattacks

1.5 million zloty
was the average cost of losses incurred by Polish companies due to hacking attacks in 2017

Reliability, security and speed **in action**

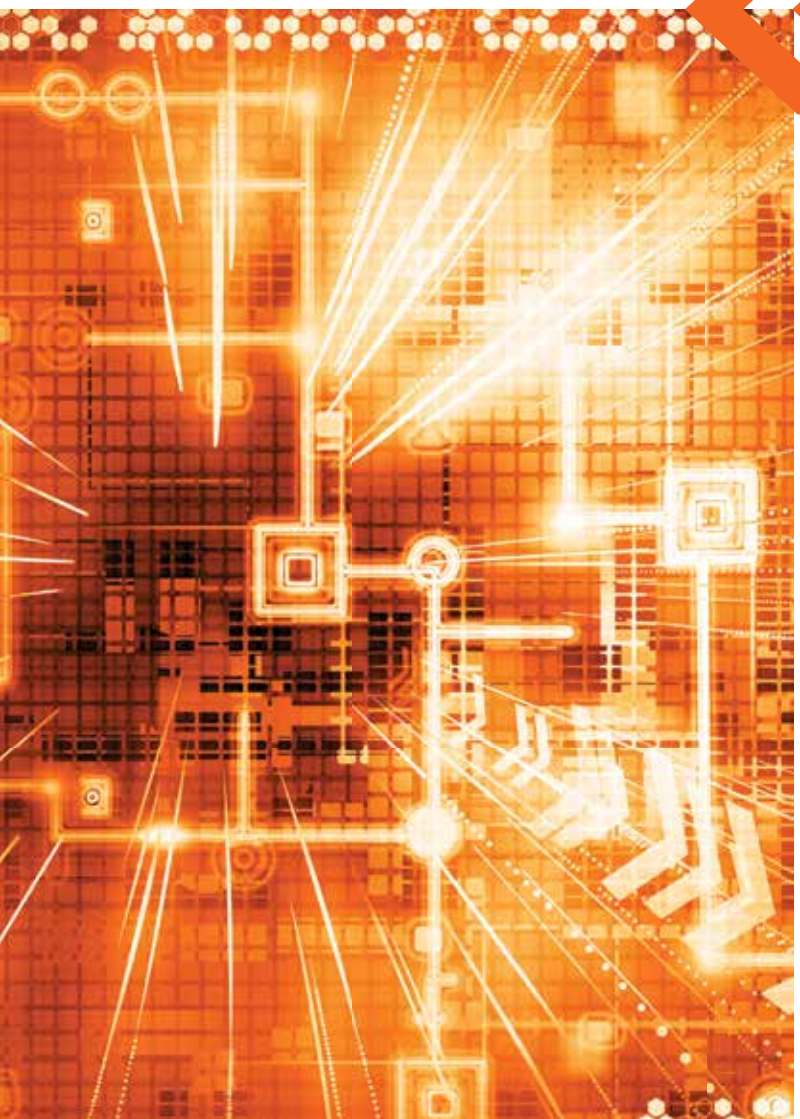
Here at Soflab Technology, we benefit from the expertise of specialists to provide IT security solutions which answer the main challenges faced by organizations today. Concern about the safety of IT solutions and the data they contain has become critical for ensuring the data security of business, as well as its continuity.

- prevent economic loss
- protect your brand from losing reputation
- manage risk
- determine the actual security level of your organization
- respond to complex threats
- fulfill the requirements of compliance with law

Testing techniques

As part of the testing process, both manual and automatic testing techniques will be used, complementing one another:

- **We use various automatic tools,** such as Nessus, Burp Proxy Professional, OWASP ZAP, SoapUI, Metasploit, as well as our own programming framework. This reduces the risk of overlooking security loopholes by one of the programs.
- **Manual audit** consists of manually verifying applications or exposures. It is used to detect logic errors or implemented functionalities. Carrying out an attack manually allows to efficiently ignore or analyze security filters that are implemented in an application or in firewall systems.



Why **Soflab**?

know-how
based on numerous projects in
various industries

a team
of competent experts

ready-made, tested,
field-proven testing procedures

experience in choosing
the right tools and technology

our own Soflab Test Approach
testing methodology

our own Testlab for mobile
application testing devices

What do **we do?**

„The best defense is a good offense", „prevention is better than cure" – these statements can rarely be applied in a single situation. There is one exception, though: IT security.

Prevention isn't widely associated with offensive actions. However, penetration tests clearly show that **in order to protect ourselves against an attack, it's a good idea to pre-emptively attack** our own system in a controlled situation – this way we can find its vulnerabilities or configuration errors. By carrying out such a security audit, we can prevent them from being discovered and exploited by an unauthorized person.

The portfolio of **our services**

Verifying the design documentation in regard to safety considerations

We provide comprehensive compliance of every project with current legal regulations, such as **GDPR**. Having a security expert in the deployment team right from the stage of designing a solution makes it possible to avoid many mistakes. It's also an opportunity to save a lot of money at later stages of an application's or IT infrastructure's life cycle.

Penetration tests

We carry out penetration tests, that is to say controlled attempts at breaching security features. Depending on clients' needs, the tests are performed with no prior knowledge about the details of the system's design **(black-box testing)**, with only partial knowledge about it **(grey-box testing)**, as well as testing which involves code examination **(white-box testing).**

Our security tests are based on the following standards: OWASP (Open Web Application Security Project), especially the OWASP Top 10 Classification; OWASP ASVS (Application Security Verification Standard) and OWASP Testing Guide 4.0 (including best practice in security testing).

We perform **mobile application security tests** using emulators as well as physical mobile devices, based on the TOP 10 Mobile Risks vulnerability and threat ranking by the OWASP organization.

Auditing the security configuration of infrastructure and individual systems/services

We conduct the audits **using manual techniques and automatic tools**. The process consists of the following elements: analysis, verification, an approach to configuration, checking the security configuration using automatic tools, risk analysis based on results, and recommendations for security optimization. The features subject to testing are: permissions, unauthorized access, configuration and missing improvements.

Information infrastructure security audit

We perform penetration tests, vulnerability scanning, we also examine the configuration of key **elements of information infrastructure**, all as part of the audit.

The testing process concerns: networks and subnetworks, network devices, hosts and network protocols, TCP and UDP ports, system platforms, network services and more..

A wide range of deployment methods includes:

- identifying the topology of a network/server;
- testing the detected network devices;
- testing wireless networks.

How do **we do** it?

Every wall can be broken through – it's just a matter of time and skill. There's always some risk. The main goal of our service is to minimize it.

- **We identify the vulnerabilities** of the company and its systems to intentional and unintentional security incidents.
- **We assess the ability to detect and withstand typical attacks.**
- **We help** in determining the **critical changes or actions in the domain of security and in the preparation of a security-ensuring action plan in the company.**

We get involved during various phases of software's life cycle – this attitude distinguishes us in the market. It allows us to support our clients at every stage of the project, plan necessary testing, identify potential threats and design project guidelines for the solution being implemented. We provide practical conclusions in a comprehensible format. The result report contains a description of the error's reconstruction, possible threats and corrective actions.

Testing the immunity to DoS/DDoS attacks

The goal is to detect weaknesses in protection against unwanted actions, leading to the blockage of web service access. We verify the most common types of DDos attacks:

UDP flood attack

It uses dedicated scripts which generate UDP packets with random sizes and time frames allocated to the estimated load.

HTTP flood attack

It's based on simulations of various methods (POST and GET) supported by an application. The generated application traffic won't correspond to the standard user but to the expected load of the resources.

Static audit of source code

Its main objective is to **identify failed design and code fragments that reflect bad programming practices or security errors**. With static code analysis, it's possible to:

- improve efficiency and stability;
- avoid common programming mistakes;
- establish coding standards and guidelines;
- increase security at every stage of testing.

The analysis is based on OWASP standards, especially the OWASP Top 10 and OWASP Mobile Top 10 classifications, as well as on the verification of compatibility with: SANS 25, HIPAA, Mitre CWE, CVE NIST, PCI DSS, MISRA and BSIMM.

Socio-technical testing, procedure and physical protection testing

Our auditors will carry out a **controlled socio-technical attack** to verify the level of security and compliance with security procedures, as well as the level of information security awareness in the organization, through tests such as:

- an attempt to persuade an employee to run software from a brought USB flash drive;
- an e-mail campaign;
- an attempt to gain unauthorized access to the building.

There's also a possibility to **provide employees with training** in information security and the latest technical and socio-technical threats.

Ask for a special offer for you:
oferta.security@soflab.pl