PENETRATION TESTS

LIREX.COM
IT INNOVATIONS

Are your systems protected from attacks?

REDUCE THE RISK WITH PENETRATION TESTS

Penetration tests mimic real attacks to systems, applications, and data that can be triggered by external hackers, malicious employees, cyber-crime organizations and others. This is a controlled, authorized process that is carried out according to the customer's requirements and in no way adversely affects the tested systems. The techniques we use allow detection of vulnerabilities that could be exploited to harm the organization. We perform the penetration tests and after summarizing the results we provide you a report containing recommendations for their resolution.

Information Security Assessment is made by:

- Identification and evaluation of vulnerabilities
- Identification of vulnerabilities that are not detected with automated vulnerability scanning
- Evaluation of the impact in case of a successful attack
- Checking the actual network security performance

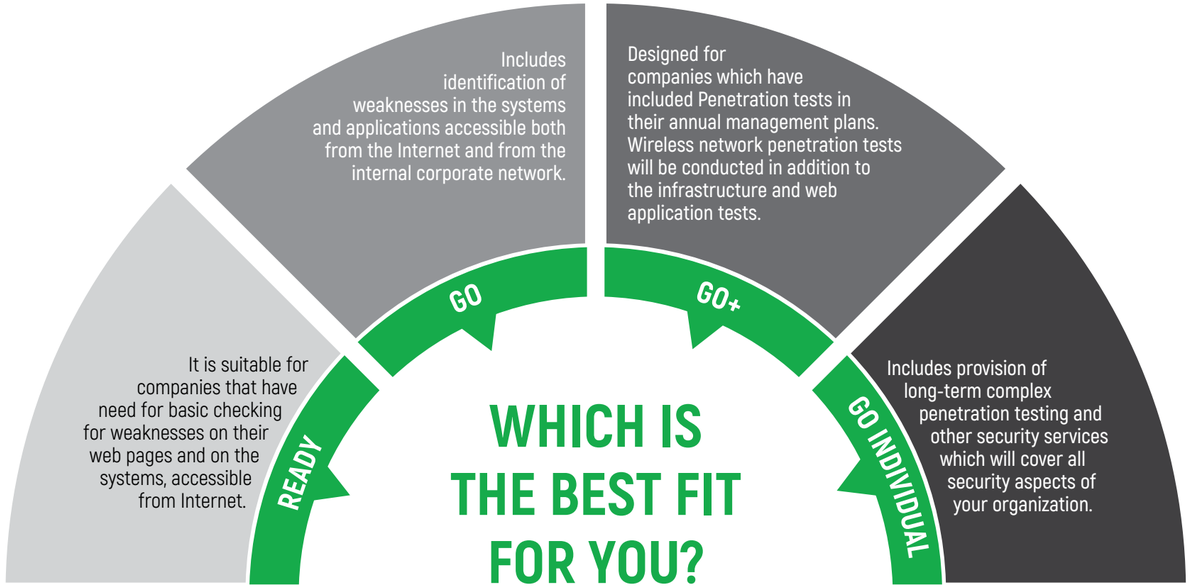
By performing more frequent and more complex tests, you can predict security risks more effectively and protect the organization from unauthorized access to critical systems and valuable information.

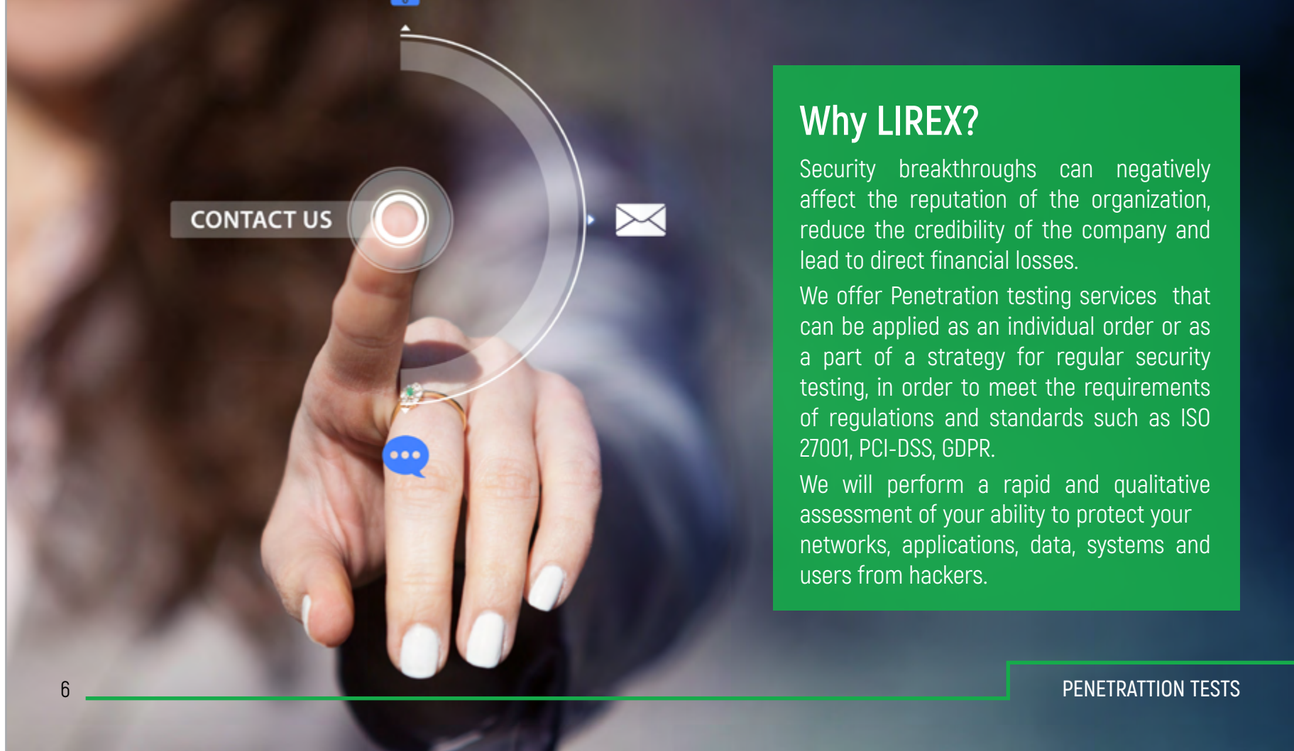
Test your IT environment

The most common attacks against information security are the attempts to compromise servers, end-point devices, web applications, wireless networks, network devices and other systems that store corporate data. We often perform tests against individual systems, such as databases, websites or internal systems which are critical to the organization. Careful planning and control makes tests safe and ensures continuity and integrity of systems and information.

Why perform such a test?

- To assess the level of protection of your networks, applications, data, systems, and users
- To protect the assets and reputation of the company by avoiding financial losses and negative publicity
- To assess which vulnerabilities are critical to the organization, which are less important, as well as to distinguish “false positives”.
- To justify the need for allocating a security budget;
- To detect vulnerabilities and enhance security in order to fit the organization systems’ criteria;
- To address basic requirements related to regulations and standards such as ISO 27001, PCI-DSS, GDPR, and prevent the imposition of high sanctions in the event of non-compliance.





Why LIREX?

Security breakthroughs can negatively affect the reputation of the organization, reduce the credibility of the company and lead to direct financial losses.

We offer Penetration testing services that can be applied as an individual order or as a part of a strategy for regular security testing, in order to meet the requirements of regulations and standards such as ISO 27001, PCI-DSS, GDPR.

We will perform a rapid and qualitative assessment of your ability to protect your networks, applications, data, systems and users from hackers.

+359 2 9 691 691
office@lirex.bg
www.lirex.bg
Mladost 3, bl.306, Sofia 1712, Bulgaria
LirexCom
Lirex COM