Orange Belgium

IT Security Solutions

Penetration Testing

Adopt and offensive approach to identify and exploit vulnerabilites in your security defense and detection systems.

Resort to *Penetration Testing* to assess your infrastructure capacity to resist to cutting-edge attack techniques.

Cyber-attacks are getting more and more sophisticated to lure advanced protection and detection solutions implemented by organizations. Consequently it's getting complicated for companies to continuously appreciate their effective capacity to face such threats. While most IT resources are devoted to ensure business continuity, fast changing threat landscape might be a challenge for them. Consequently, your teams can lack of time, expertise and familiarity to be fully aware of the latest attack methods and vectors.

Apply methodologies used by cyber criminals to access your corporate data and reduce your attack surface by identifying and mitigating vulnerabilities within your IT environment.

Most organizations have implemented sophisticated security controls and incident response plans to face the exponential growth of cyber attacks. But unless they are regularly tested for potential weaknesses, cyber criminals can exploit hidden vulnerabilities and endanger your business continuity.

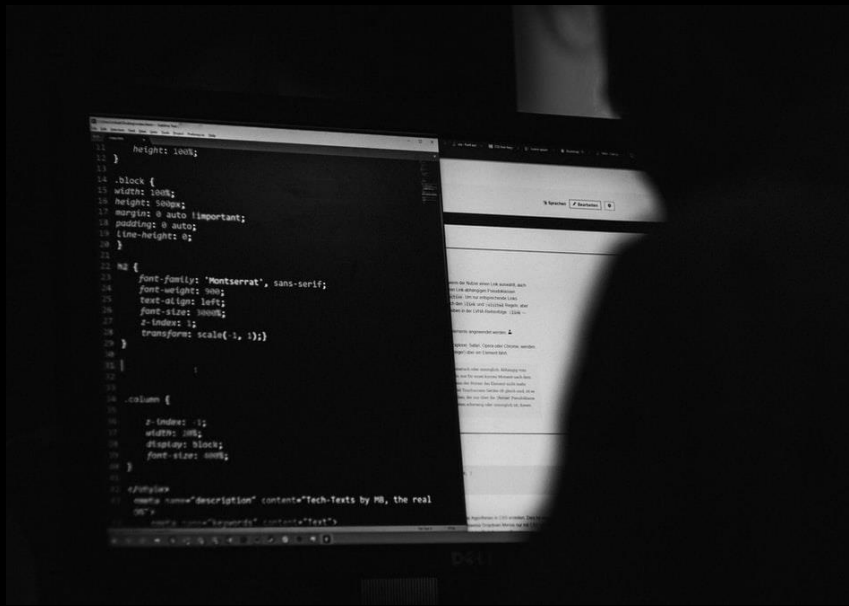
Therefore, Orange supports organisations by providing *Penetration Testing* intended to demonstrate how an attacker would gain unauthorised access to your environment by using similar tactics and techniques.

When should you perform a Penetration Testing?

- **Before a system, network or application is deployed and put in production;**
- **When your system is getting stable;**
- **After a cyber attack;**

How often?

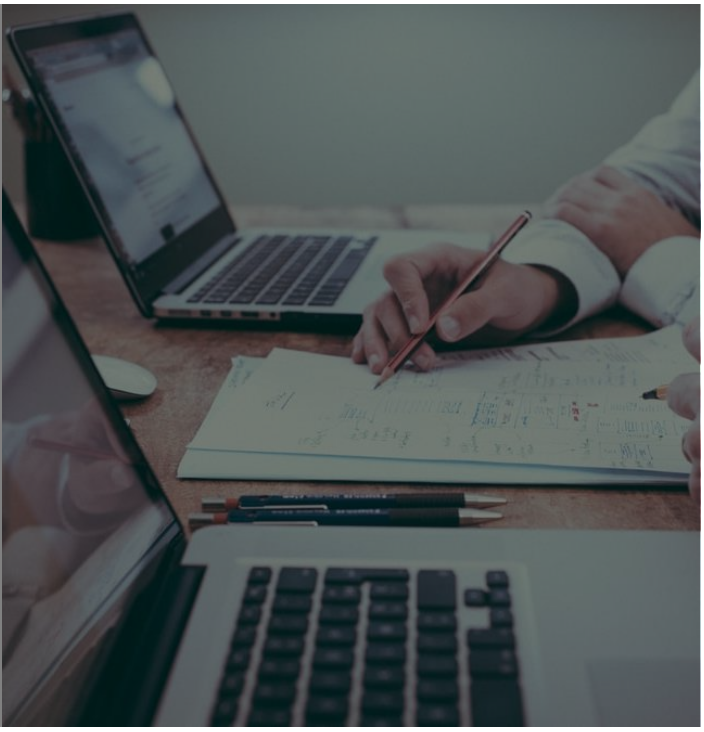
- **From quarterly to yearly depending on your exposure to cyber risks (ie. industry, online...);**
- **When a new law and regulation is published and requires security measures;**



Penetration Testing benefits

- Identify potential vulnerabilities before an attacker does;
- Provide information helping your security team to mitigate vulnerabilities;
- Improve your incident response capacities with real attack simulation;
- Provide proof of compliancy to your business partners and authorities;

How does Penetration Testing work?



Usage of **several techniques** including vulnerability scanning, exploiting of vulnerabilities, password cracking…

Supported by Orange **Ethical hackers**

In-house **methodologies** and usage of industry **standards** (ie. OWASP)

Reporting including actionable **recommendations** from our experts

Which perimeter can be addressed by a Penetration Testing?

Internal & External network

- Identify vulnerabilities of internet-accessible systems to gain access to internal resources;
- Simulate an insider activity exploiting his access to corporate data;

Web & Mobile application

- Use of the OWASP standard to assess the security of web-based applications;
- Exploit mobile device vulnerabilities;

Red Team

- Simulate a real world attack;
- Discover the weakest path to exploit a vulnerability within your infrastructure;

More information
https://business.orange.be/en/it-solutions/security-solutions

Orange Belgium
Avenue du Bourget 3,
1140 Evere

Contact us
B2BSecurity@orange.be