Types of penetration testing for businesses

No matter what your company does, how large or small it is, cybersecurity is something you need to think about and take care of on a regular basis. Thousands of businesses are targeted by hackers every day and one way to protect your business, employees and clients from cyber attacks is by conducting regular and rigorous penetration testing. High-quality penetration testing can protect you from potential future hacker attacks, which can cost you millions in lost revenue, downtime, fines from government agencies because of compliance problems, damage to your reputation and more.

What is penetration testing?

Even if you've put a lot of effort and resources into ensuring that your company is safe against cyberattacks, you can never forget about hackers for a long time. The field of cybersecurity and the hackers' toolbox are always evolving, so it is necessary to regularly examine your networks and systems to ensure that there are no vulnerabilities. A penetration test does just that - during penetration testing cybersecurity specialists examine your company's servers, networks, devices, applications and more to find potential points of attack for hackers. All the issues then need to be fixed to keep your business safe from potential security breaches.

Penetration testing types

Network penetration testing

One of the most common types of security testing is network penetration testing. During this type of penetration testing, security specialists simulate an attack on a company's devices, hosts, systems and networks to identify weak points that hackers can exploit. Once these vulnerabilities are identified, the level of risk presented by them is assessed and the vulnerabilities are fixed.

Application penetration testing

Application penetration testing refers to the security testing of software, web and mobile applications. Cybersecurity experts try to compromise the software, gain unauthorized access to different parts of the program or take it over completely. This type of testing should always be done by a third party when developing an app or program for in-house or commercial use, as people who develop the software often can't see all the potential security flaws.

Physical penetration testing

Physical penetration testing is conducted not on wireless networks or devices, but on the company's actual premises. This type of testing examines how an intruder can gain access to

sensitive areas of buildings or grounds. This testing involves an assessment of motion detectors, alarms, cameras, locks and other physical security devices.

Social engineering penetration testing

Finally, the last type of penetration security testing assesses the risk of security breaches due to human error. Experts use social engineering to assess the cybersecurity awareness and preparedness of certain employees at a company and attempt to gain access to their personal information, passwords and accounts through manipulation and false pretenses.