

Penetration Testing

Reports of data breaches surface each day yet we're regularly surprised by the scope of many breaches and the involvement of supposedly "impenetrable" organizations. You may think your infrastructure is protected, but those with malicious intent are continuously looking to exploit vulnerabilities. While vulnerability scans and automatic updates reduce the risk of an external or internal party causing harm, the only way to know how your infrastructure would react in the event of an attempted attack is to conduct penetration testing.

Penetration testing, the examination of security vulnerabilities and attempting to exploit them, is a key line of defense for protecting organizations from breaches. It is a critical component of a robust information security program which every organization should conduct regularly. PCI DSS requires organizations to annually conduct both internal and external tests. Starting Jan. 31 2018, service providers using network segmentation to reduce the scope of their PCI environment must additionally have a penetration test to validate their network segmentation conducted every six months.

An internal penetration test originates at the company and involves attacking the system from the inside. An external penetration test tries to gain access via the internet, breaking through firewalls. TECH LOCK employs "ethical hackers" -trained certified experts -to search for weaknesses in infrastructure (hardware), applications (software) and people.

Penetration test results help organizations proactively correct deficiencies before you experience a breach.

"The Standard for Data Breach Prevention."

TECH LOCK Can Help You Pinpoint and Address Your Security Weaknesses

Examining security vulnerabilities and attempting to exploit them is a key line of defense in protecting your organization from breaches.

Having a third-party validate the security controls in place and providing findings for improvement drives security efficiency with actionable remediation steps.

With annual penetration testing, or with major technology changes, organizations can quickly improve their overall security posture.

There are a wide variety of penetration tests available, each assessing different aspects of your organization's cybersecurity. TECH LOCK can perform the following types based on your goals and needs.

White Box Testing is when the tester begins with full knowledge of the target, including firewalls .

Black Box Testing is when nothing is provided beyond the organization's name.

Gray Box Testing is when a limited amount of information is available.

Network and Host, penetration tests include network and host penetration testing as standard.

Web Application penetration testing includes identifying and exploiting SQL injection flaws and combining with other methods such as social engineering in cross-site scripting and cross-site request forgery attack.

Social Engineering involves human interaction. Examples include phishing emails and telephone calls used to obtain credentials and access to internal systems.

Premise and Physical Security, a network can be technically secure but physically vulnerable. Regularly testing physical security controls can be just as important as a network penetration test.

TECH LOCK STRENGTHS

In addition to their extensive experience as penetration testers, TECH LOCK security engineers also possess deep technical knowledge as IT professionals making them uniquely qualified to identify any security weaknesses and provide solutions to ensure a successful remediation.

- Several types of penetration tests are available.
- Testers hold industry-leading certifications, including SANS GPEN and Offensive Security.
- Experienced security engineers go beyond automated testing and seek out vulnerable spots in systems finding and reporting new exploits.
- Tests are designed to determine risk and report on the potential business impact, reporting that quickly makes sense for those holding security leadership positions.
- Rules of engagement are carefully defined to provide a professional and safe penetration test with proper level of notification and defined scope.

