Saisystems TECHNOLOGY

From the Saisystems Technology Blog

What SMBs Need to Know Before Conducting a Penetration Test

Hackers attack every 39 seconds, on average 2,244 times a day. With the increased adoption of remote work, having a resilient and reliable network is more critical than ever. Penetration testing, or pen test, is the most efficient method of uncovering and addressing vulnerabilities before being exploited. The value of pen test, however, is not limited to patching your security. When done properly, penetration testing can build a scalable IT organization. It's easy to commence a penetration test, but what you do with the generated data determines your test's real values. Don't jump into penetration testing without these expert insights on how and when SMBs should build their pen test cadence.

What is penetration testing?

Penetration testing is the method of checking a computer device, network, or web application for security bugs that an attacker might exploit. Penetration testing may be done manually or with the aid of software programs. The procedure entails collecting information about the target before the evaluation, determining potential entry points, trying to break in, and reporting the results. A network pen test's general testing methodology includes 5 phases: Network reconnaissance, Service Discovery, Vulnerability Identification, Vulnerability Exploitation and Vulnerability Rating. Each stage is built upon the previous one to measure your network's efficacy and provide a complete view of gaps and blind spots.

Penetration testing is beyond identifying immediate vulnerabilities

The primary goal of penetration testing is to find security flaws. Penetration testing can also help evaluate a company's security policies, conformity to regulatory standards, employee security knowledge, and ability to detect and respond to security events. Key insights that a company can gain from penetration testing:

- Strengths and conditions of the current system
- Fulfillment of regulations/ standard compliance
- Impact of an intruder's attack
- Effectiveness and accuracy of intrusion detection
- Effectiveness and accuracy of the response systems

These insights cover the full spectrum of your network security and inform both business and policy decisions. Data discovered by penetration testing is compiled and distributed to an organization's IT department to allow the organization to fix problems and make policy choices, making it crucial to organizations that deal with shared networks. Such organizations can conduct penetration testing as a means to measure the true efficacy of their technological controls. For small and medium businesses (SMBs), the result of pen test is beyond uncovering immediate threats and vulnerabilities. With finite resources, organizations need to be smart in choosing which vulnerabilities to address first. A key result to look for in pen test is prioritizing risks based on severity, exploitability and scope. No two organizations are the same. There is no common framework of prioritization across the board. Cybersecurity analysts can build a testing and action plan catered to the specific context of your organization. This is also the reason why many SMBs struggle with building a good penetration testing cadence. The lack of dedicated IT personnel and tools makes it difficult for organizations to flag vulnerabilities and address them timely. Look for a third-party vendor like Saisystems who can support you with immediate risk mitigation and proper documentation and build a scalable long-term strategy to uplift your IT security.

When do you need to conduct a pen test?

Penetration testing requires coordination and clear communication across the team to minimize disruptions and maximize insights generation. More importantly, penetration testing is not a once-and-done activity. As your company scales, so do the threats that you face. Regular pen testing ensures your security can support your business expansion and can scale as your IT organization grows.

These are the triggers that signal the need for penetration testing:

- You have reached a milestone in your development of software or system implementation
- You have applied changes in applications, systems, network or process
- You deployed new infrastructure. Areas of deployment includes software development, app, or security.
- You need to recover from a security incident or have reached a milestone in a remediation project
- You need to build a compliance/audit mandate
- You are running a vulnerability management program that entails penetration testing.

Meet one of these conditions?

The next step is to find a trusted partner to help you test your system efficiently and cost-effectively.

Contact us to find out how to start your customized penetration testing strategy.

Not ready for penetration testing yet?

Risk assessment might be a better option for starters.

Our complimentary assessment can help you identify security gaps and jumpstart your cybersecurity project.

203-929-0790 | info@tech.saisystems.com | www.saisystems.com/tech/

Saisystems TECHNOLOGY