digitaldefense
by HelpSystems

Penetration Test Pitfalls to Avoid

While pen testing has been around since the 1960s, not all organizations have perfected the art of conducting them. In fact, not all companies are taking advantage of them, but that's a conversation for another time. Below are a few common pitfalls that even experienced security teams fall victim to from time to time.

Wrong Frequency

Testing only once a year or so may not be enough, especially during times of digital transformation or transition. While some IT governance and compliance mandates require an annual penetration test frequency, there are certain events that could be considered triggers that warrant additional tests. These include the application of large security patches, the instillation of new infrastructure & the addition of physical locations or a relocation of your network.

Not Your Type

The wrong type of pen test will fail to address the controls your business deems most important. To understand which type of pen test suits your needs best, you must determine how your business prioritizes risk associated with infrastructure, web applications & people.

Depending on your answer, you may need a network penetration test, a web application penetration test, a social engineering test or all the above. Be sure to prioritize your areas of concern appropriately and take common attack vectors and potential damage into account.

Disastrous DIY

Pen testing requires finely tuned ethical hacking expertise. Done incorrectly, pen tests can create more problems instead of just identifying those that exist. It's best to identify a trusted vendor that can help you configure and conduct regular tests simply and painlessly. Be sure the vendor you choose specializes in pen testing and keeps abreast with the latest hacking techniques.

Noisy Reporting

The point of pen testing is to ultimately emerge better informed than you were when you began. Unfortunately, many penetration testers provide clients lengthy reports of indigestible vulnerability data, creating confusion and more work for teams that are typically already over tasked. Find a vendor that provides straight forward reporting that helps prioritize high-risk, critical vulnerabilities.

Tunnel Vision

Many organizations conduct penetrations tests for the sole purpose of compliance, resulting in limited tests that fail to uncover potential vulnerabilities. Cybercriminals are cognizant of these requirements and won't hesitate to try to infiltrate areas that might be ignored by limited tests. It's best to concentrate on assessing and prioritizing areas of risk for your business to inform your testing.

Failure to Finish

Surprisingly, many organizations fail to organize and complete the remediation, rendering the pen test meaningless and a total waste of time and money. Prior to testing, come to a consensus on the remediation strategy. Time is of the essence, because the longer an issue lingers, the more likely it is to be exploited.

Learn more about Digital Defense Penetration Testing.