Penetration Testing

What is Penetration Testing?

A Penetration Test (or Pen Test) is the process of identifying security gaps in your IT infrastructure by mimicking a real-world attacker. Pen Testing typically falls within three categories: Black Box, Gray Box and White Box. Black Box testing provides the tester with virtually no information about the target system. Gray Box testing typically involves a minimum amount of system information including user level credentials. White Box requires the tester have full access and explicit knowledge of the target system. Pen Tests can be performed both internally and externally and are designed to provide vital insight into the security posture of your network.

Why Should Penetration Testing Be Performed?

Recent statistics place the global average for a data breach at $3.86 million. That amount more than doubles if you are within the United States. In addition to financial loss, there are intangible losses such as damage to a company's reputation and subsequent loss of business which are much more difficult to quantify. In today's technology-driven environment, eliminating 100% of risk is impossible, but performing routine Pen Testing is an essential part of identifying and addressing security risks with the goal of improving overall IT security posture. The reasons for conducting pen testing could range from proactive assessment to meeting compliance or regulatory requirements such as PCI DSS, HIPAA, NIST, etc. As the owner of your customer and employee data it is critical you understand your overall security posture and close any gaps attackers may take advantage of to disrupt or gain unauthorized access to your environment.

How Does TechGuard Approach Penetration Testing?

Prior to a Pen Test engagement, we will develop mutually agreeable rules of engagement to ensure expectations from both parties are fully defined. Items such as dates/times of the assessment, systems in scope, escalation paths and contact information for all parties are included. TechGuard Security follows the National Institute of Technology and Standards (NIST) methodology (NIST SP 800-115) for pen testing. The process generally follows a four-phase methodology consisting of Planning, Discovery, Attack & Exploitation and Reporting. Our consultants attempt to find vulnerabilities and weaknesses using various pen testing tools and techniques, both automated and manual. Once the assessment has been completed, we will conduct a collaborative, high level presentation of the assessment performed. We will review critical and high-level findings and discuss recommended remediation actions. We will also follow up with an actionable, prioritized findings report which will be complete with remediation and/or mitigation recommendations.

What is the TechGuard Difference?

We pride ourselves in building and maintaining long-term relationships with our clients. This ensures each client receives a tailored, customized service based on their unique organizational needs. From the initial kickoff meeting to delivery of the finalized Penetration Test Report, client satisfaction is our number one concern. At TechGuard, we place the utmost value on the delivery of quality services. Every client is assigned a Project Lead who will serve as their single point of contact throughout the engagement. In addition to the detailed written report provided at the end of the assessment, clients engage in a presentation with their Project Lead. Our report delivery presentation provides the opportunity to discuss details of important action items, next steps, and answer any questions related to remediation recommendations. TechGuard has dedicated the past 18+ years to delivering high-end, professional cybersecurity solutions - making us a trusted partner in both the government and private sectors.