Healthcare Penetration Testing Levels

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

A Healthy Approach to IT Security

Attackers who venture to breach networks and steal data will search for weaknesses to exploit in the software, services, or systems that exist on those networks. By thoroughly testing a network's defenses in order to identify security weaknesses, administrators can remediate vulnerabilities before an attacker is able to exploit them. Security best-practices and regulatory bodies either recommend or require regular penetration testing to ensure organizations are aware of weaknesses. Many cybersecurity breaches are crimes of opportunity and can be avoided if vulnerabilities are identified and properly secured before a breach occurs.

To combat these threats, TraceSecurity created 3 Levels of Penetration Testing to meet the needs of healthcare organizations of all sizes and types.

Level 1

Level 1 is a remote External Penetration Test (EPT) which demonstrates how vulnerabilities found on network devices provide pathways through which an attacker could gain access to devices and the private data available on those devices. When requested by examiners and auditors, the EPT report provides proof that the client if performing penetration testing as recommended by most regulating bodies.

Level 1 includes:

External Penetration Test (Remote)

Level 2

Level 2 includes an External Penetration Test and an Internal Penetration Test performed remotely. This testing is designed to demonstrate how technical vulnerabilities - present on either the internal or external network - can provide pathways through which an attacker could gain unauthorized access to devices and private data present on those devices.

Level 2 includes:

External Penetration Test (Remote)
Internal Penetration Test (Remote)

Level 3

Level 3 was designed to demonstrate how vulnerabilities can provide pathways through which an attacker could gain unauthorized access to devices and private date on those devices, These vulnerabilities may be technical in nature or exploitable via social engineering. The Level 3 Penetration Test aims to identify both types of vulnerabilities with both remote and onsite testing, and provide recommendations for addressing any findings.

Level 3 includes:

External Penetration Test (Remote)
Internal Penetration Test (Onsite)
Qualys PCI Scan and Report
Onsite Social Engineering
Wireless Assessment & Penetration Test
Clean Desk Review
Dumpster Dive (Main Facility)