With cyber-attacks on the rise, businesses need to realize the importance of information security and take necessary steps to improve their defense. A part of this defense includes the testing of your security controls. But what type of tests do you require and at what times? Let’s talk about three different types of security assessments i.e. vulnerability assessments, penetration testing and security audits. These do not replace each other. Your security policy should include a strategy that integrates all three types of security assessments.

**Vulnerability Assessment**

A vulnerability assessment analyzes your system devices, software applications and operating systems to identify underlying vulnerabilities. This may include devices that have firmware with known vulnerabilities, outdated software, and others. This security assessment is often carried out by using automated vulnerability scanning tools. When a scan is completed, it includes recommendations such as to patch software or update devices.

Software programs continuously have detected vulnerabilities, and it’s very important to keep one’s system updated. Vulnerability assessments are easy to automate and have lower costs. Due to this fact, it’s affordable to conduct these scans regularly.

While this type of security assessment is good for identifying vulnerabilities, it does not attempt to actually exploit the detected vulnerabilities. In order to do so, penetration testing is required.

**Penetration Testing**

Penetration tests simulate an attack as it happens in the real world. A tester attempts to not only identify but also exploit vulnerabilities in your system. This test can use a combination of known misconfigurations, vulnerabilities and weak prevention mechanisms for identifying risks missed by any other type of security assessment.

A penetration test also enables you to evaluate your intrusion detection and monitoring capabilities. Its scope can vary widely, and depends upon the parts of your system that you want to evaluate. Penetration test has different types, based on how much information you provide to a tester. In a black-box test, you do not give any information and the tester will need to identify potential targets by themselves. In a grey box test, you give part of information to the tester, mainly to speed up the whole process. A white-box test involves the testers having complete access to the target.

**Security Audit**

This type of security assessment involves evaluation of your security controls against a specified set of standards such as ISO 27001, HIPAA or PCI DSS. It mainly focuses on how well you have developed and implemented security policies and procedures.

If you are wondering about how to conduct a security assessment for your business, contact Aardwolf today for consultation and specialized security assessment services.