**How Often Should You Perform a Network Vulnerability Scan**

A network vulnerability scan is a part of your vulnerability assessment process. The main focus lies in identifying security vulnerabilities in the systems that are hosted on particular IP addresses. Though every business has different needs, the general best practice is to perform a network vulnerability scan once every quarter. However, you may require vulnerability scans every month as a result of changes in infrastructure, compliance requirements, or internal network security capabilities. A vulnerability scan helps identify and close down attack vectors by giving details such as vulnerabilities found, potential exploits and mitigation recommendations.

**Factors Determining the Frequency of a Network Vulnerability Scan**

The need for conducting vulnerability scans relies greatly on how willing you are as a company to commit to information security best practices.

Some of the major factors that determine the frequency of vulnerability scans include the need to achieve and maintain:

* **Compliance:** Many security standards require companies to conduct regular vulnerability scans. Most audit processes include presenting of quarterly assessment and remediation reports to the auditors.

Some well-known compliance standards include:

* + ISO 27001 – It is one of the most widely accepted certification standards in information security. It recommends conducting internal and external vulnerability scans on quarterly basis.
  + Health Insurance Portability and Accountability Act (HIPAA) – Though, it does not require network vulnerability scan, it places a lot of emphasis on vulnerability and risk assessment, which can be easily identify with a vulnerability scan.
  + Payment Card Industry Data Security Standard (PCI DSS) – This standard has strict requirements in terms of network vulnerability scan. It requires qualified personnel of an approved scanning vendor to conduct quarterly internal and external scans.
  + National Institute of Standards and Technology (NIST) – NIST is not a standard but a framework for organizations to develop their cyber security program. Many information security officers use NIST guidelines to incorporate into their program for strengthening their security controls. Depending upon the NIST framework (800-53, 800-171, etc), you require vulnerability scans monthly or quarterly.
* **Effective Vulnerability Assessment Process:** For every information security program to be successful, it is vital to have an effective vulnerability assessment process. Hence, it’s important to mitigate identified vulnerabilities and contribute in overall safety of the organisation’s network and systems.

Once you identify the vulnerabilities, it takes approximately one to two weeks to apply proper mitigation measures to address the issues. Hence, a follow-up scan with same configurations is recommended after applying the fixes to validate the success of the mitigation actions.

* **Security after a Major Change in Infrastructure:** Conducting vulnerability scans after major infrastructural changes is a common practice. A scan must also be done after a major deployment of software. This is not an easy process and requires one to do a lot of careful work without disrupting everyday business activities. However, conducting a network vulnerability scan ensures that you have not missed anything in the new implementation.

If you would like to find out more about how often your organisation needs to perform network vulnerability scans, contact Aardwolf Security for a consultation.