Organisations that prioritise security must keep vulnerability management at the top to establish a clear approach for identifying issues affecting their systems. A vulnerability scan is a major component of vulnerability management. It allows you to evaluate your system, infrastructure and software for unpatched loopholes that require remediation. Let’s have a look at some best practices for vulnerability scanning that can help businesses protect their assets.

**How Often Should We Perform Vulnerability Scanning?**

This depends upon a number of factors such as compliance standards, organisational changes and your security program objectives. If your organisation plans to maintain high security level, vulnerability scanning must be a part of your information security program. A vulnerability scan should be carried out after any major organisational, system or infrastructural changes to ensure the prevention of security gaps.

You also need weekly, monthly, quarterly or annual vulnerability scans to comply with various security standards such as ISO 27001. Generally, it is considered best practice to perform vulnerability scans once every quarter. It allows organisations to identify major security vulnerabilities for assessment. However, you can also perform the scans monthly, depending upon your organisational needs. The best way to determine the frequency requirement of your scans is to understand your threats and security structure thoroughly.

**What Compliance Frameworks to Consider?**

When complying with security frameworks, you will see that most of them have mandatory requirements of regular vulnerability scans. Some of them require you to conduct vulnerability scanning more frequently than others. Some of these regulatory standards and their requirements are as follows:

**ISO 27001:** It requires quarterly internal and external vulnerability scanning

**Payment Card Industry Data Security Standard (PCI DSS):** It requires quarterly scans conducted by an Approved Scanning Vendor (ASV)

**Health Insurance Portability and Accountability Act (HIPAA):** It requires a detailed risk assessment and vulnerability management, which includes vulnerability scanning.

**National Institute of Standards and Technology (NIST**): It requires monthly or quarterly vulnerability scanning that depends upon the framework i.e. 800-53, 8001-171, etc.

**How to Conduct Vulnerability Scanning?**

Vulnerability scanning is often confused with penetration testing. However, it serves a different purpose. Contrary to penetration testing, vulnerability scanning is an automated process that identifies issues in a system at regular intervals. We can conduct a vulnerability scan with a number of tools.

We at Aardwolf Security, provide vulnerability scan services with the best tools. Expect a thorough scan of your system, networks and equipment for detecting and classifying vulnerabilities. If you are interested in learning more about our services, contact us today by clicking here.