VULNERABILITY MANAGEMENT CHECKLIST

Vulnerability management is a crucial security measure followed in organizations. The process discovers, assesses, and remediates the vulnerability loophole prevalent in your network and protect from cyberattacks.

In order to get the vulnerability management right and make the best out of it, you need to ensure that your vulnerability management program meets the following requirements.

Get Complete visibility and control over your entire IT infrastructure

"You cannot protect what you cannot see", as this popular saying goes, you should have complete visibility over your IT infrastructure. You should be aware of all your network devices, endpoints, servers, applications installed on each device, services, processes, ports, user login details, and everything that is a part of your IT infrastructure.

Classify and update your IT asset inventory

Businesses use IT assets for different operations. There are in-house assets, third-party assets, and public/private cloud assets. You need to assign risk levels to these assets based on the crucial business area they support. You can assign the risk value based on the business operations they support, the sensitive information they carry, and the transactions that take place in these assets. This type of classification will help while planning your security strategy.

Make vulnerability management a continuous process

Many organizations look at vulnerability management as an audit process and periodically follow it in their network. These organizations run vulnerability scans only once or twice a month and take even more time to remediate them. New vulnerabilities are discovered every day, and exploits possibilities increase each day. Hence, make sure you practice vulnerability management as a continuous and ongoing process.

Perform both internal and external assessments continuously

Internal and external assessments are crucial to identify vulnerabilities that can impact your business. External scans look for holes in your network firewall that let attackers break and exploit your network. Whereas internal scans identify the real and potential vulnerabilities prevent inside your business network. You need to perform both these assessments continuous to get an inside out picture of your network's vulnerability exposure.

Identify solutions that provide security coverage for your entire IT infrastructure, including network devices, end-points, and applications

It is not sufficient if your vulnerability management solution offers coverage only for endpoints or applications. Vulnerabilities exist everywhere in the network. You must lookout for a solution that provides vulnerability coverage to your entire IT infrastructure. The solution's security feed should support vulnerabilities across all network devices, endpoints, different types of operating systems, and an array of applications.

Rely on scanners that detect vulnerabilities more accurately

Not all vulnerabilities have a CVE number or are a part of the NVD database. More than 40% of vulnerabilities are not listed in the NVD database and do not have any CVE identifier. Relying only on CVE data while discovering vulnerabilities will give a false sense of security. Ensure that you opt for a vulnerability scanner that supports all vulnerabilities irrespective of CVE data.

Do not depend on unauthenticated scanning techniques

In the earlier days, the unauthenticated scanning technique was popularly used to secure external facing assets. However, the scanning result was insufficient for the security teams to plan their remediation tasks. Unauthenticated scanning lacks the breadth and depth of vulnerability coverage, and in most cases, do not cover even 30% of vulnerabilities present in your environment. This limits the vulnerability discovery and lets down the whole vulnerability management program. Hence, opt for authenticated scanning for accurate detection and greater visibility.

Look at vulnerabilities and risks holistically

It is difficult to name only a specific security flaw as a vulnerability. A vulnerability could be anything in a network like application and OS vulnerabilities, vulnerabilities in network devices, misconfigurations, deviations in system settings, old network protocols, weak passwords, account enumerations, publicly shared devices and folders, outdated operating systems and applications, unpatched devices, firmware & software, enabled guest logins, un-updated antivirus, unwanted services and processes, usage of rogue applications, and much more. There are 100 security flaws that will pose a huge risk to your organization security. You need holistically look at all these vulnerabilities and manage them effectively to prevent attacks.

Prioritize vulnerabilities based on risk

If you end up with a pile of vulnerabilities in your network and randomly start remediating them, there are chances you might focus your efforts on the less critical ones. It is always essential that you prioritize the vulnerabilities based on their severity range before planning remediation. By this, you can quickly eliminate the vulnerabilities possessing high risks.

Plan your remediation strategy wisely

Once you have prioritized the vulnerabilities in your network, you can smartly plan your remediation strategy. Plan and remediate the vulnerabilities with the most critical risks first, followed by the less critical ones.

Automate vulnerability remediation

Automate the vulnerability remediation process in your network to remediate the critical vulnerabilities on time. Taking manual methods to patch critical vulnerabilities will take a long time and might leave enough security gaps for the attackers. Automate patching in your network to remediate vulnerabilities quickly.

Test your patches in the test environment first

Some patches that vendors release may be faulty and cause software disfunction and system behavioral errors. Hence, testing the patches in a test environment is always important before deploying them in the production environment. Ensure that you create a small test set up replicating the systems in the production set up and test the patches there.

Go beyond patching to remediate all vulnerabilities

Patching is not the only remediation measure to mitigate vulnerabilities. As mentioned, vulnerabilities should be looked at holistically and their remediation measures. You should opt for a solution that provides remediate beyond patching to uninstall software, quarantine systems, stop services and processes, block applications and devices, harden system configurations, run scripts, and much more.

Assess and reassess mitigations

After successful mitigation of vulnerabilities, assess the results thoroughly. Make sure that the mitigation technique has bought down the vulnerability count in your network. If not, make effective changes to your mitigation process to increase the effectiveness of your vulnerability management program.

Develop compliance reports adhering to the industry's popular benchmarks

Vulnerability management is the most recommended security measure by various industry compliance benchmarks like HIPAA, PCI, ISO, and NIST. While managing vulnerabilities in your network, create reports adhering to these benchmarks as they will come in handy during the compliance audit times.

Automate the entire vulnerability management cycle

Vulnerability management is not a one-step process. Automate the entire cycle from detection, assessment, prioritization, remediation to reporting to tighten the security in your organizations. Automation will save time and resources and increase the overall effectiveness of the vulnerability management program.

About SecPod:

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on computing environment. Our product helps implement cyber hygiene measures so attackers have tough time piercing through.

Our SanerNow CyberHygiene platform provides continuous visibility to computing environment, identifies vulnerabilities and mis-configurations, mitigate loopholes to eliminate attack-surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better, everyday.