How to Manage Security Vulnerabilities

Vulnerability management leverages a set of workflows and products designed to sustain the IT infrastructure, testing it for security flaws and fixing the vulnerabilities detected. This is an ongoing routine denying the notorious approach of not fixing things that are not broken. The latter approach just fails to meet modern protection demands. Unless reviewed and enhanced, the digital assets are easy to compromise.

Scanning does not suffice

In contrast to the scanners detecting security flaws, vulnerability management aims at reinforcing IT infrastructure protection and enabling rapid response to specific critical perils. Spotting a vulnerability is essential, yet measures must follow to quickly prevent the attackers from accessing the system through the detected loophole once and for all. The techniques assessing security vulnerabilities and ranging the flaws identified within the customer's infrastructure are critical to apply. Scanning alone fails to provide these features.

Vulnerability management boils down to expanding the scanning routines as it assesses, prioritizes, and patches the spotted flaws. Clients' demands are changing. If earlier the main goal used to be to spot a vulnerability, now it is more about how to solve the problem.

Licensing models

As regards the licensing approaches implemented by the systems designed for security vulnerability management, they are based upon the number of IPs to be protected. Their location or the installation count does not matter. The price for a scanner that detects security flaws, on the contrary, is subject to the number of installations and the scanning presets, such as the number of host systems to be monitored.

Besides, installation modes differ as certain providers make their products available for unrestricted usage. The functionality provided also defines the costs to be incurred as certain options are provided as paid extras.

How to pick up your best system for vulnerability management?

First off, pay attention to how big your organization is, how many offices it has within each time zone, and whether the product is subject to localization as that defines the ability to identify security flaws related to a specific area or industry.

An essential factor is the ability of IT and security units of the organization to discuss and finalize the list of functions to be provided by the vulnerability management system. Security experts tend to focus on identifying security flaws, and IT departments usually prioritize the deployment of patches. It is thus the merge of the vulnerability detection and patch management that determines the final parameters of the vulnerability management solution.

Besides, pay attention to whether the updates are conducted in full, how often you have updates, and what operating systems are supported. A perfect tool for managing security vulnerabilities is to be within the profile of the activity the company is operating and the software products it is using.

When signing the contract, the system provider would want to persuade the client that the solution will get new services and options in the future. However, this is not always the case as some vendors do not follow this routine. So, you should focus on the already included vulnerability management system features.

Any vulnerability management solution would improve its performance by using verified third-party vulnerability databases. It is also good if the system could come up with a specific malware that exploits a given security flaw.

Most organizations deal with a common choice of whether they stick with free vulnerability scanners or purchase a full-fledged vulnerability management solution. Maintaining a vulnerability database is a challenge involving significant expenditures and effort. As a result, a non-paid solution calls for the developers to focus on alternate activities to get revenues, which is why the functionality of such products is restricted.

Solutions involved in vulnerability management workflows

The kit of tools required to arrange the management of security flaws within an organization may comprise as follows:

- Various solutions for collecting data about vulnerabilities, for example, scanning software, as well as vulnerability databases.
- Instruments prioritizing the detected flaws in line with the Common Vulnerability Scoring System (CVSS) standard.
- Tools managing the security flaws within the company, its sub-systems, as well as the worldwide distribution of the attack.

Patching vulnerabilities and managing assets

The company asset management performs best when ongoing. It should use the automation of the highest level and be applied to the whole IT infrastructure. Prioritizing security vulnerabilities is not feasible without observing the above requirements. Besides, you cannot manage the infrastructure unless you know precisely what it comprises. That is, asset management is critical for managing vulnerabilities.

The critical condition for establishing automatic patch management is a unique identifier to be set for each security vulnerability and ensuring the upcoming system update is patching it. That is a sophisticated workflow; its implementation involves many challenges. Omitting just one update might have dramatic impacts. All patches should be done neatly and strictly.

Besides, aligning automatic patches with specific application areas is essential. In the case of PCs, the updating can be limited to common apps such as office software, browsers, and OS. For servers, the situation is more challenging as the stakes are too high, and a corrupted patch can render unavailable the assets that the organization must have access to.

As regards the business infrastructure, organizations tend to scan rather than introduce agents on the devices to be protected as those endpoints too often serve as ports for malware infiltration. Nevertheless, if there is no other method for interfacing with the end host, you should apply a data collection agent.

Again, good cooperation between IT and security teams is critical. These departments need to set up the rules they mutually recognize and explicitly assign responsibilities for updating specific assets, as well as the frequency of those updates. In a nutshell, a good security vulnerability management workflow is to boil down to ensuring such conventions are complied with and critical patches get installed instantly.

Prospects for the vulnerability management market

The market is now clearly shifting towards automating the patching and asset monitoring routines. While corporate IT facilities keep on moving into the cloud, there is a good chance that vulnerability scanning will come down to monitoring the parameters of cloud security. The other trend is towards the enhancement of the systems for gauging the severity of the security flaws. Vulnerability prioritization systems are going to process more significant amounts of information, in particular the data related to the vulnerabilities that the attackers exploit most.

It is also within the realm of possibility that such tools will implement the all-inclusive approach in the upcoming years so that one tool will provide the full range of IT security features. Such a comprehensive suite managing risks, vulnerabilities, assets, and patches and providing other security options is quite likely to emerge. There will likely be a universal vulnerability management platform comprising all aspects of the IT infrastructure, from a container on a managed hosting service to a printer.