feature

Enterprise Vulnerability Management

Today's enterprises have solutions in place to help with the detection and management of their information systems vulnerabilities, especially as it relates to system software and firmware. These vulnerabilities can be anything from a bug in the code that allows attackers to gain root access or even an update flaw that might fix one vulnerability, but cause another vulnerability. Some of the challenges enterprises encounter are viruses, malware, spam and phishing schemes. Multiple tools are available that can assist with detecting vulnerabilities throughout all enterprise systems. Each tool has pros and cons. With the availability of so many options, IT professionals need to have a firm grasp on their definition of vulnerability, how to manage particular vulnerabilities and the types of solutions that will best fit their enterprise.

Vulnerability Management Tools

A vulnerability management tool helps to discover and identify anything that is attached to the enterprise network (the enterprise assets). The assets can include firewalls, computers and tablets. The tool also identifies the operating system and the applications running on the asset. After gathering this information, the tool then assesses those applications and devices for vulnerabilities. It establishes a baseline or a snapshot of where the most risk and vulnerabilities currently exist so that it can inform the administrators of the vulnerabilities that must be fixed or patched to ensure that a system/application is safe to run. Although all vulnerability management tools have different advanced features, they all have the same basic processes—discovery, prioritization and remediation/mitigation.[1, 2, 3]

Discovery determines all of the assets that are connected to the network and if they have any vulnerabilities. The prioritization process evaluates the vulnerabilities and their associated assets, and ranks them on severity level. Usually, the ranking is from one through five, with five being the most critical. Remediation/mitigation is the process that provides a list of recommendations to address the vulnerabilities and vendor patches for the assets.

IT professionals should conduct proper research on the available vulnerability management tools to find the appropriate tool for their enterprise. The key functions to look for in a tool are automated scanning and alerting. Although many tools might have these features, some might not be able to perform these steps automatically. Another key function is the tracking of vulnerabilities over time for the enterprise. This tracking helps to ensure that these vulnerabilities are being patched as soon as possible, whether it is by the vendor or by internal IT staff. The ability for someone with administrative capabilities to run a scan on a deeper level, i.e., to gain more information than someone who does not have administrator credentials, is another important feature. Ease of use is also important when considering tools. IT professionals should look for a tool that performs the tasks they want without having to spend many hours trying to learn the system and customizing features to make it usable for the enterprise, i.e., a tool that has a fairly easy setup and can start functioning as quickly as possible.

Trevor J. Dildy, CCNA
Is a member of the East Carolina University (ECU) (North Carolina, USA), classroom technology team, which is responsible for researching state-of-the-art hardware and software for ECU classrooms. Previously, Dildy was a member of the information technology security team at Vidant Health, assisting with access administration requirements for the health system.

When choosing a vulnerability management tool, it is important to take into account how often the system requires maintenance, including upgrades to newer versions, updates to individual features, and patches to any weaknesses or loopholes in the programming. When choosing a tool, it is of vital importance to determine if end users of the assets will notice a decrease in performance during maintenance operations. If scanning must occur during normal business hours, end users cannot experience any sort of performance reduction on the systems, such as freezing, loss of connectivity or crashing. Due to increased use of the cloud and mobile devices, it is beneficial if the selected tool has options to run in the cloud or from mobile devices. This is useful if a user of the tool cannot be at his or her workstation to initiate a scan when something occurs or if the user chooses to use the tool while on a mobile device. Although mobile and cloud options are ideal to have, they are not required to have a very useful vulnerability management tool and should not deter enterprises from purchasing the best tool for their organizational structure.

Other Vulnerability Management Solutions

Other solutions bring new and useful ideas to vulnerability management. The four essential capabilities (and steps) of vulnerability management (VM) are network discovery, scanning, reporting and correlation, and asset prioritization.[4] VM tools fall into three broad categories: appliances, software applications and cloud services.

Appliances are devices that can easily scan headquarter environments or large regional offices because of their ability to scan large networks quickly. This kind of advantage comes at a big price.

Software applications can be either commercial or freeware, which makes it a bit more difficult to have the system ready right out of the box. For example, freeware has an open license, which can cause issues due to no hardening of the system.

Software applications can have a much lower cost than appliances; however, additional configurations are required for software applications before this type of tool is able to function properly. It requires customizing the operating system (OS) and making sure that the OS is secure and not vulnerable to outside attacks.

Cloud services are a low-cost alternative to appliances and software applications, but cloud services come with a risk. To scan internal IP addresses with cloud services, it is crucial that a device is deployed to scan assets on the network. If the device is not an option, then the alternative is to place huge security gaps in the firewall. This alternative should not be used when sensitive information resides on the enterprise network.

Ensuring True Vulnerability Management

Ensuring that vulnerabilities are addressed quickly and efficiently is crucial. The numerous vulnerabilities that are discovered every day can interfere with the proactive process of keeping enterprise systems patched and updated. Vulnerabilities are not the only issues with vulnerability management. Poor change management practices, rogue servers and blurred network boundaries also cause issues with practicing true vulnerability management.

“When choosing a tool, it is of vital importance to determine if end users of the assets will notice a decrease in performance during maintenance operations.”

Information Management

One way to ensure that true vulnerability management is achieved is to have proper information management. Typically, when it is time to relay information to people during an incident, it is up to the computer security incident response team (CSIRT) to manage the information. Because the CSIRT is usually aware of the state of security for the enterprise, it can double as, or work with, the vulnerability management team. The CSIRT is able to guide the vulnerability management team with planning for patches and other processes.

Risk Assessments

Risk assessments are another way to help determine the state of vulnerability management within the enterprise. Risk assessments determine the amount of risk that particular systems pose to the network. Executive management can use this information to determine which of those assets should be patched first or if any systems can afford to absorb the risk associated with them. However, it is difficult to give a new vulnerability a risk rating without knowing how this risk will affect the network-connected assets.

Vulnerability Assessment

True vulnerability management requires a robust vulnerability assessment (VA). Numerous freeware utilities are available to conduct VAs, such as nmap or a paid utility such as Nessus.[5, 6] These tools help the vulnerability management team discover vulnerabilities within the network. It is necessary that experienced security professionals work with freeware utilities for effective vulnerability assessments. Inexperienced personnel can cause more harm than good to the network. It is necessary to get permission from change control to run vulnerability assessment scans. Some of these tools can cause network disruption, so it is crucial to not run these scans during periods of heavy network usage. Although vulnerability assessments can be time consuming, they can save the enterprise from a major breach caused by a vulnerability.

Vulnerability assessments can also assist with the functionality of intrusion detection system (IDS) and intrusion prevention system (IPS) tools. Integrating vulnerability assessments with the IDS/IPS can help by adding more details to alerts and preventing false alerts from occurring.[7] Alerts that give more detail about what is occurring on the system can clarify the severity of the discovered vulnerabilities and help the enterprise develop a better plan of action.

Ensuring proper threat-level assignment can help with managing the vulnerabilities to the enterprise. The threat-level assignment should be easy for the team to understand and in a visual and/or numeric representation of the current threat level.[8] **Figure 1** shows five levels of threat assignment, from severe to low.

After threat-level assignments are defined, vulnerability management countermeasures and controls can be developed to help prepare the enterprise for each level of threat. When the vulnerabilities have been identified, controls can be put into place to help mitigate the risk that those particular vulnerabilities create.

“Although vulnerability assessments can be time consuming, they can save the enterprise from a major breach caused by a vulnerability.”

Reporting and Remediation Tracking

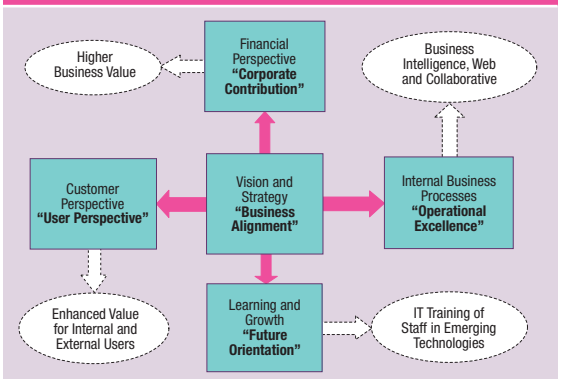
Another step that can be added to the four vulnerability management steps (network discovery, scanning, reporting and correlation, and asset prioritization) is reporting and remediation tracking.[9] This additional step ensures that all vulnerabilities are reported and remediation steps are taken. Even if remediation is not necessary because the enterprise has chosen to absorb the risk, it is important to keep proper documentation on the particular vulnerability in case it develops into a greater risk or issue in the future. Vulnerability assessments help to speed up penetration testing for the enterprise; a penetration test can help to confirm whether the vulnerabilities are serious and detect the presence of disputed vulnerabilities.[10]

Figure 1—Threat-Level Assignment
Severe/5/Red Attack in progress or imminent Incident response team should be activated
High/4/Orange Attack behaviors and activities identified in information infrastructure Vulnerability management countermeasure plans should be initiated
Elevated/3/Yellow Evidence of attack capabilities and motivated adversaries identified Controls should be reviewed for effectiveness
Guarded/2/Blue Attack possible, but not likely Information infrastructure monitors should be tuned to possible attacks
Low/1/Green No current evidence of attack capabilities or motivated adversaries Vulnerability management plans should be reviewed and updated

Source: T. Dildy. Reprinted with permission.

Producing a scorecard to map vulnerability management with risk management is essential to aligning IT governance to corporate goals and objectives. **Figure 2** shows how a balanced scorecard is mapped to an information technology scorecard. An enterprise can alter the scorecard to reflect the enterprise organizational structure.

Figure 2—Balanced Scorecard Mapped to IT Balanced Scorecard



Source: Kapur, R.; "Use of the Balanced Scorecard for IT Risk Management," *ISACA® Journal,* vol 5, 2010, *www.isaca.org/Journal/archives.* Reprinted with permission.

BYOD Strategy

When developing a vulnerability management strategy, devices that are not owned by the enterprise should be included, and a plan to address them should be developed. Bring your own device (BYOD) is common practice in many enterprises, and many users of these devices are not technology savvy or aware of the many potential vulnerabilities that their devices present. Although device owners may see the vulnerability management of their devices as a nuisance or an inconvenience, it is essential. If device owners want to use their personal devices onsite and on the enterprise network, a scan of their device needs to be done. If the device does not have the latest updates or patches installed, the device owner must install them immediately or be denied access to the network. This BYOD strategy is the primary method to prevent someone's personal device from opening the network to outside attackers. Keeping the network safe from devices that have not been updated or patched is the best way to make sure that there is all-around vulnerability management.

Intelligence

A key component of vulnerability management is intelligence.[11] Conducting proper research and

gathering information about vulnerabilities that affect other enterprises is key to having a well-designed vulnerability management plan. Making sure that all of the proper information is gathered about the current and known vulnerabilities helps the enterprise prepare for when an attack does happen. This intelligence ensures that everyone is prepared for the attack and can help to reduce the impact or help to reduce the risk's impact on the enterprise.

> **"Although device owners may see the vulnerability management of their devices as a nuisance or an inconvenience, it is essential."**

Numerous tools are available to help with vulnerability management. All of these tools are useful in their own way and can deliver important information to any enterprise, but these tools alone cannot ensure that enterprises are doing all that they can to make sure their network-attached assets are safe from vulnerabilities. Although these tools can help to detect the assets that are connected to the network and those that need to be patched, it is up to the vulnerability management team to determine which of these vulnerabilities need to be patched. The CSIRT is an asset that enterprises cannot afford to be without if they would like to have effective vulnerability management. This team has the best understanding of the security that is currently in place within the enterprise, which is very useful when it is time to conduct vulnerability assessments.

Making sure to gather the appropriate amount of information on the current threats that are affecting other systems can help to develop the proper plans and make sure everyone is prepared to combat a vulnerability if it is discovered on their system. Most enterprises want to do all that they can to manage vulnerabilities as they occur, while understanding that not every vulnerability can be patched.

Endnotes

1 Tittel, E.; "Introduction to Vulnerability Management Tools," TechTarget.com, January 2016, *http://searchsecurity.techtarget.com/feature/Introduction-to-vulnerability-management-tools*

2 Tittel, E.; "Seven Criteria for Buying Vulnerability Management Tools," TechTarget.com, January 2016, *http://searchsecurity.techtarget.com/feature/Seven-criteria-for-buying-vulnerability-management-tools*

3 Tittel, E.; "Comparing the Top Vulnerability Management Tools," TechTarget.com, February 2016, *http://searchsecurity.techtarget.com/feature/Comparing-the-top-vulnerability-management-tools*

4 Fortinet Inc., "Vulnerability Management for the Distributed Enterprise," 2010, *https://www.yumpu.com/en/document/view/20912289/vulnerability-management-for-the-distributed-enterprise-fortinet*

5 Lyon, G. F.; *Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning*, Insecure.Com LLC, USA, 2008

6 Nessus Vulnerability Scanner, *https://www.tenable.com/products/nessus-vulnerability-scanner*

7 Hammons, K.; "Vulnerability Management is Not Simple," ISSA, 2014, *https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0214.pdf*

8 Pironti, J. P.; "Key Elements of a Threat and Vulnerability Management Program," *ISACA® Journal*, volume 3, 2006, *www.iparchitects.com/wp-content/uploads/Key-Elements-of-a-Threat-and-Vulnerability-Management-Program-ISACA-Member-Journal-May-2006.pdf*

9 Brackin, C.; *Vulnerability Management: Tools, Challenges and Best Practices,* SANS Institute, 15 October 2003, *https://www.sans.org/reading-room/whitepapers/threats/vulnerability-management-tools-challenges-practices-1267*

10 *Op cit,* Hammons

11 *Op cit,* Pironti