EITS
Enterprise IT Security

RELEASE DATE:	CONTACT:
November 18, 2020	John Davis
	Sr. Security Architect
RELEASE METHOD:	Enterprise IT Security
Social Media and Website	info@eits.com

How to Implement a World-Class Vulnerability Management Program

What is Vulnerability Management?

Simple! It's just managing vulnerabilities, right? It's literally right there in the name!

Actually, vulnerability management is a continuous, cyclical process that often involves multiple technology teams. There are five elements to vulnerability management: 1) asset discovery, 2) vulnerability identification scanning, 3) vulnerability evaluation and prioritization, 4) patch/configuration remediation, and 5) reporting. Vulnerability management, when implemented alongside other security tactics, is vital for an organization's security posture. Appropriate execution of a vulnerability management program prioritizes possible threats and minimizes their risk of successful attack. Why is this an iterative process? Vulnerability management needs to be performed continuously in order to keep up with new devices being added to the network, changes being made to devices, and the discovery of new security vulnerabilities. Security vulnerabilities are a technological weakness that allow a malicious actor to manipulate an IT component to perform actions that are not intended. As you can see, there's a lot to learn about vulnerability management.

I have more than 15 years of career security experience, including security networking, engineering, architecture, policy, and, yes, vulnerability management. Early in my IT and Security career, while researching the best way to perform vulnerability management, I memorized NIST SP 800-40 Version 2.0 (DOI) "Creating a Patch and Vulnerability Management Program" and NIST SP 800-40 Revision 3 "Guide to Enterprise Patch Management Technologies". Given the great NIST resources on this topic, one might ask, "Why waste time writing about vulnerability management?" The answer is simply that I have yet to find the perfect vulnerability management program. Vulnerability management is one of the most basic security fundamentals, but it is almost impossible to master; this is because there is not a panacea for vulnerability management.

Why is Vulnerability Management so Difficult?

The main reason vulnerability management is so difficult is that it is so resource intensive; successful vulnerability management requires technological, financial, and human resources. Many organizations employ a vulnerability scanning tool to identify known exploits in their infrastructure and a separate tool to update software packages, but the significant time and resources that are required to maintain other aspects of the vulnerability management process are not allocated appropriately. Human elements, such as muddied communication and unclear ownership, also contribute to stalled, ineffective vulnerability management programs.

How to Properly Implement a Vulnerability Management Program

I've played an active role in shaping vulnerability management programs at several different organizations throughout my career; using the knowledge I've gained, I am going to discuss what worked and how other programs fell short. The easiest way to do this is to begin by describing the purposes of each of the five elements of vulnerability management.

1. **Asset Discovery**

   Identifying and classifying all hardware and software inventory is the critical first step to vulnerability management. If you don't know something is there, you can't manage it. The Center for Information Security (CIS) has a Top 20 list of critical controls that many organizations do not perform effectively. The top two controls on this list are hardware inventory and software inventory; this certainly isn't a surprise. Asset discovery is not only important, it is consistently the most difficult task to "wrap arms around," regardless of an organization's size or complexity. Constant vigilance is imperative; to have a successful vulnerability management program, it is critical to continuously monitor for new devices on the network. Just monitoring for these devices is not enough, however, as it is also critical to identify changes to the software installed on these assets. Even the slightest software configuration change can have a big effect on overall security.

2. **Vulnerability Identification Scanning**

   The second step, vulnerability identification scanning, builds on asset management. Once all of the hardware and software that comprise the technological environment have been identified, scanning the environment for vulnerabilities can be automated and generally requires the fewest amount of human resources dedicated to it. It is critical to ensure that all assets are being scanned and that the scanner can properly assess the system; this requires that the scan is performed with administrative credentials or an agent can be installed on the system. Performing port scans is an important part of vulnerability identification to ensure that new vulnerabilities have not been added from unauthorized configuration changes.

   If some systems on a network become unstable or behave erratically when scanned, then the application owner should work with the vendor to address the issue. Vulnerability scanning should not result in a denial-of-service for properly configured applications. During the initial implementation of a vulnerability management program, assets might need to be excluded from vulnerability scans, but this is not a tenable long-term solution.

   Performing regular, continuous vulnerability assessments over time enables organizations to understand the speed and efficiency of their vulnerability management. Vulnerability management solutions have various options for exporting and visualizing vulnerability scan data; these options include customizable reports and dashboards. This helps IT teams easily understand which remediation techniques will help them fix the most vulnerabilities with the least amount of effort and helps security teams monitor vulnerability trends over time in different parts of their network. Customizable outputs also help support organizations' compliance and regulatory requirements.

3. Vulnerability Evaluation and Prioritization

After vulnerabilities are identified, they need to be evaluated so that the risks posed by them are dealt with appropriately and in accordance with an organization's risk management strategy. These risks can change based on the information accessible on the system, the network placement of the system, or the business criticality of the system. Vulnerability management solutions will provide different risk ratings and scores for vulnerabilities, such as Common Vulnerability Scoring System (CVSS) scores. These scores are helpful in telling organizations which vulnerabilities they should focus on first, but the true risk posed by any given vulnerability depends on some other factors beyond these out-of-the-box risk ratings and scores.

Vulnerability evaluation requires three things: teamwork, teamwork, and more teamwork. Business requirements combine with security risk factors to determine the priority a vulnerability poses to an organization; a qualified security professional needs to analyze the vulnerability scanning results to ensure they are valid and to help prioritize the remediation focus. Knowing which vulnerabilities to fix first is critical, especially when starting a vulnerability management program; however, this is often the most misunderstood step in the vulnerability management process. The business side of an organization must be committed to transparent and timely communication. As silly as it sounds, it is also imperative that the business understands what information is stored on their assets and how these assets communicate to each other. If there are business processes that are a high priority or if the business is adding hardware and software, it is imperative that the security team knows this. Similarly, the security team must engage in consistent education and outreach. If members of the business team do not understand the "why" of security, they may not understand the value of working closely with the security team. Additionally, it can be a challenge for organizations to validate new vulnerabilities because the security team generally does not have administrative access to infrastructure systems to verify the validity of new vulnerabilities.

I have captured many of the questions that need to be answered to properly prioritize vulnerabilities below:

- Is this vulnerability a true or false positive?
- Is the asset directly exposed to the Internet?
- What is the age of the vulnerability?
- How difficult is the vulnerability exploit?
- Is the exploit proof of concept code available for the vulnerability?
- What would be the impact to the business if this vulnerability was exploited or if the asset was unavailable?

- Are there any compensating security controls in place that reduce the likelihood and impact of this vulnerability being exploited?

4. Patch/Configuration Remediation

The patch remediation phase involves implementing changes to correct the previously discovered vulnerabilities. This phase is almost always handled by a different team than the previous phases, which makes communication critical. Most organizations have a security team who would have been leading the vulnerability management process until now, and a team of IT specialists for networking, infrastructure, and operations. The IT specialists will almost always be the team that operationalizes the patch/configuration remediation plan. For this reason, it is also critical that the team applying the software updates is in sync with the team performing the vulnerability scanning; otherwise, the result is a disjointed program that leaves gaps in the security posture. Since each vulnerability is different, it is important that the remediation team test their work before it is deployed to production.

Vulnerability management solutions provide recommended remediation guidance. Occasionally, a remediation recommendation is not the optimal way to remediate a vulnerability; when that happens, the right remediation approach needs to be determined by an organization’s security team, business owners, and IT administrators. A relatively common example of this is that a patch is not available; in this instance, the security team should apply compensating controls as an alternative while reaching out to the vendor for an update. Remediation can be simple, such as applying a readily available software patch, or complex, such as implementing new infrastructure.

5. Reporting

The reporting phase helps identify the success of the vulnerability management program. A successful vulnerability management program will include several executive-level reports as well as more detailed reports for the security and patch teams. Since vulnerability management is such a time and resource intensive process, it is important that progress is reviewed with an organization’s Executive management. Developing the correct reports can be challenging; it is critical to accurately report on the state of the vulnerability management program, while also ensuring that erroneous information is filtered out.

Using reporting to understand a security program’s effectiveness means calculating, communicating, and comparing key metrics. When used appropriately, reporting can give an organization the data needed to track a Cyber Exposure Score (CES), the time to assess, and the time to remediate and compare those metrics internally and against industry best practices. Once results have been analyzed, communicate them – sharing with key stakeholders will build confidence in your program's success.

How does Vulnerability Management Go Wrong?

In my opinion, the number one reason that vulnerability management programs are not successful is because the program does not have upper management buy-in. Vulnerability management programs are guaranteed to fail without this continued support. In my experience, this is the case even if all the steps provided in this article are followed. If the vulnerability management program doesn't have VP (or higher) acceptance to clarify that the vulnerability management effort is a priority, then it's just an unimportant waste of resources.

I would list the second leading cause of disfunction in a vulnerability management program to be the lack of ownership and responsibility. It is critical that IT, security, and the business subject matter experts are identified for each asset. Vulnerability ownership can be tricky because most standard vulnerabilities will be the responsibility of the patch team, but certain application-specific vulnerabilities should be managed by the application owner. The best vulnerability management program that I have been involved with had a website dedicated to tracking vulnerabilities that was checked daily by the IT technicians; the IT technicians could then filter vulnerabilities that they were responsible for based on their infrastructure. If the vulnerability was assigned to them, but was not their responsibility, then they could reassign the vulnerability to the asset owner. This process ensured that the correct owner had vision into what vulnerabilities were their responsibility.

Another problem in vulnerability management programs is poor communication. It is critical that the security team scanning for new vulnerabilities and the team fixing the vulnerabilities are in constant communication. It can be very frustrating when new vulnerabilities randomly appear; this is especially frustrating if management does not understand why the new vulnerabilities appeared and blame the patch team. I have often seen frustration on the security team as well when vulnerabilities are not addressed in the timeframe outlined in the security policy. It is important that the security and patch teams have regular communication to ensure that both teams understand the status and priority of current outstanding vulnerabilities.

Another common problem I have observed in vulnerability management programs is bad reporting. There is nothing more frustrating than exerting a bunch of effort to resolve an issue and having someone else undermine that effort. It is critical that vulnerability management reports are split to show past-due vulnerabilities as well as upcoming vulnerabilities that need to be addressed. In my experience, a well-run patch team will remediate the majority of vulnerabilities before the vulnerability is visible to management. It is important that these vulnerabilities are included in a report to show the overall success and hard work of the patch team. While each vulnerability is different, it is important that the correct owner is assigned to ensure accurate reporting.

The final common problem I have observed is scanning assets with appropriate credentials. While there is some minor value in performing uncredentialed vulnerability scans, the majority of vulnerability scans should be performed with administrative credentials on the asset. Granting the vulnerability scanning tool administrative access is the only way for the tool to properly recurse through all of the installed software and determine the truly exploitable vulnerabilities on the system.

Conclusion

I like to think of certain IT and security functionalities as being either “cornerstone” or “capstone” – in other words, there are some aspects of a comprehensive security program that must exist before anything else can be created, and there are some aspects that can only be added after the program is mature. Vulnerability management, being integral to computer and network security, is a cornerstone functionality. The five elements of vulnerability management must be performed methodically and with complete transparency and full buy-in from all the verticals involved.