10 Steps for Achieving

Effective Vulnerability Management

Table of Contents

The Challenges for Vulnerability Management

FOR EVERY ORGANIZATION, information is a valuable asset, yet it is challenging to secure. As the value of information increases so too does its attractiveness to criminals and other attackers. However, unlike other valuable assets such as cash, information is not secured in a large safe which can be easily protected. Instead, information is spread across many systems, networks and devices, exposing it to the possibility of it being compromised.

Adversaries attempting to steal information range from traditional hackers looking to compromise a system, to online activists looking to promote their causes, to criminals monetizing the data and systems they compromise, to corporate- or state-sponsored spies seeking valuable information. Though these tools and techniques employed by these different groups range in sophistication, they all rely on weaknesses in the system (e.g., missing patches, poor passwords, system misconfiguration). Given the rate of change in organizations today and the range of software employed, the odds are heavily in favor of the attackers finding vulnerabilities.

The word "vulnerable," according to the Oxford English Dictionary, means "exposed to the possibility of being attacked or harmed"

The traditional approach to vulnerability scanning is to scan systems and applications for weaknesses at certain intervals. These intervals might be quarterly or monthly scans, for example. The problem with this approach is that the organization only has visibility of the vulnerabilities detected at those particular points in time and if the scanning process isn't integrated with other processes within the organization, it might miss new systems that are added to the network, new vulnerabilities that have been discovered, or other items that leave the organization with an incomplete picture of the vulnerability landscape they need to manage.

What is required is a comprehensive vulnerability management program tightly coupled with other essential operational security processes

The word "vulnerable," according to the Oxford English Dictionary, means "exposed to the possibility of being attacked or harmed". An effective vulnerability management program should therefore look at ways to reduce the possibility of systems being exposed to harm. This requires a more comprehensive view of how to manage vulnerabilities than simply scanning systems and reacting to the results. What is required is a comprehensive vulnerability management program tightly coupled with other essential operational security processes, such as coordination and communication across groups, asset management, patch management and incident response.

Identifying Key Weaknesses

THERE ARE A NUMBER of areas that can expose systems to harm. Some of these areas include:

Software

All software inherently has bugs. Some of these bugs may never be discovered and the software may continue to function perfectly. Other bugs may cause performance or aesthetic issues. Some bugs lead to security weaknesses which if exploited can impact the confidentiality, the integrity, or the availability of that software or the data within that system. Most vendors regularly release updates to their software to address bugs. Keeping software updated with the latest releases is a key element in ensuring the security of systems.

Keeping software updated with the latest releases is a key element in ensuring the security of systems.

Implementation & Configuration

Another step in securing systems is to ensure that systems are implemented and configured correctly. However, some systems may not be set up securely or their configuration may change as a result of ongoing maintenance or troubleshooting. Implementation and configuration issues like having certain insecure services running, using default or weak passwords, or not switching diagnostic functions on a production system could all cause security vulnerabilities.

Changes

The nature of modern computer systems is that they regularly change. These changes could be the result of a planned activity such as an upgrade, the addition of new functionality or to aid in the troubleshooting of a problem. However, if these changes are not managed, they could introduce vulnerabilities into the environment. A key element in dealing with these security challenges is the ability to have a constant overview of the current state of these systems and the rapid detection and identification of any new vulnerabilities.

Human

A key element often overlooked in securing a network is the human element. Most people simply see the computers, applications and networks they use as tools to help them do their job. However, if they are not properly trained in the secure use of the systems, they can expose these systems to security threats. People may use weak passwords, turn off security software to improve the performance of their computers, install software from an unauthorized source, or change the configuration of their computers to suit their own needs. Regular monitoring of key systems and the people who use them can identify potential vulnerabilities.

Regular monitoring of key systems and the people who use them can identify potential vulnerabilities.

Often the cause of a security breach can be attributed to a vulnerability arising from one or more of the above areas failing, with no way to monitor, detect and/or repair that failure. An effective vulnerability management program will have strong scanning program as its base, and also integrate with other processes and workflows throughout the organization to maintain an overall strong security posture.

10 Steps for Achieving Effective Vulnerability Management

TO ENSURE IT CAN PROACTIVELY DETECT and respond to security threats, an organization needs to implement a comprehensive vulnerability management program that is integrated with other disciplines. This allows vulnerabilities to be detected early so that other processes, such as patch management, protect the organization from a potential breach.

The steps to take to create a modern, effective vulnerability management program include;

Step	Why?
1. Asset Identification and Management	Identify all the assets that need to be secured
2. Vulnerability Identification	Know the vulnerabilities that exist for each asset and their severity
3. Consistent Vulnerability Management	Scan frequently, identify problems, implement fixes and repeat
4. Risk Assessment	Determine the value of each asset and the level of security needed to protect it
5. Change Management	Identify and deal with security issues when change happens

6. Patch Management	Include the value of assets to the organization as a factor in determining how software updates are applied
7. Mobile Device Management	Manage mobile and transient devices for vulnerabilities
8. Mitigation Management	Manage vulnerabilities that have no patches or fixes
9. Incident Response	Proactively respond to incidents and potential incidents
10. Automation	Reduce the time to detect, assess and remediate vulnerabilities

Asset Identification and Management

In order to secure something it is important to first know that it exists, what it is and where it is located. A crucial first step in securing a network is to identify all of the assets on that network. These assets should include every element that makes up the computing environment, such as routers, switches, servers, firewalls, printers operating systems, system software, and application software.

A crucial first step in securing a network is to identify all of the assets on that network

The relationship and dependencies between various assets should also be identified and recorded. Recording the relationship and dependency between assets makes it possible to determine the path an attacker could take to compromise an asset. This helps determine the criticality of any vulnerabilities identified against an asset. The asset with the vulnerability may not be of high value to the organization; however a high value asset may be connected to the vulnerable asset which would impact how that vulnerability would be managed.

Identifying and recording assets as they connect or disconnect to the network is key to ensuring a consistent view of all vulnerabilities. If an organization's network is static, where devices are not regularly connected or disconnected from it, it may be possible to manually record these devices. However, most networks are not static and devices such as laptops are regularly connected and disconnected. In this situation, ways to automatically detect devices as they are connected to the network will need to be employed. These could range from:

- Using a Network Access Control system to manage devices connecting to the network.
- Reviewing the logs on the DHCP servers on the network to determine what devices have been assigned an IP address.
- Regular reviews of the DNS server logs will also identify devices looking to communicate on the network.
- Installing vulnerability scanning agents on those assets and have them scan and report back to a central vulnerability manager on a regular basis.

Vulnerability Identification

Knowing what vulnerabilities exist for each asset and the criticality of that vulnerability is essential in determining how best to secure it. Vulnerabilities may exist on each device and asset due to missing patches, old software, weak passwords, or poor configurations. How easy it is to exploit that vulnerability, or the damage that could be caused by exploiting the vulnerability will determine its criticality.

Understanding the criticality of discovered vulnerabilities enables organizations to prioritize resources needed in mitigation efforts.

Consistent Vulnerability Management

A point in time vulnerability scan will only provide a limited view of the potential security exposure. Any new vulnerability introduced as the result of newly discovered software bugs, new devices added to the network, or changes to systems will go undetected until the next scan, leaving those systems at risk until those vulnerabilities are identified. Less frequent scans can also result in large numbers of vulnerabilities to address after each scan. In some cases, the sheer volume of

vulnerabilities discovered can discourage any remediation action.

Using consistent, high-frequency scanning enables an organization to quickly identify any new vulnerability. It can also reduce the volume of vulnerabilities from any one scan, making it more likely that those issues will be addressed.

Risk Assessment

Not all devices and assets will require the same level of security. Depending on the value to the organization of the asset and how exposed it is will determine what steps are required to protect it. Risk is often described as the impact an attack will have, balanced by its likelihood of occurrence and the complexity of success. Vulnerabilities are what allow an attacker to find an entrance in an otherwise protected environment. A weak password runs the risk of being easily guessed and allowing unauthorized access to the system. A missing patch on a web server runs the risk of an attacker exploiting that vulnerability to gain access to the server.

Not all devices and assets will require the same level of security

To make informed risk management decisions on the levels of risk posed

against an organization's information assets requires accurate and timely details on the vulnerabilities that exist. Employing a consistent vulnerability management approach provides timely data to support an effective risk management process.

Change Management

Changes occur regularly on many networks and systems. Software is upgraded, hardware is added or removed, and applications are constantly updated. Each change has the potential to introduce new vulnerabilities or issues that could undermine the security of the organization.

Integrating change management with a consistent vulnerability management process will ensure potential security issues are identified and dealt with earlier.

Patch Management

An effective vulnerability management program should be integrated tightly with the patch and release management processes to ensure that

software updates are applied to systems and assets in accordance with their criticality to the organization. Feedback from the patch management program should be given to the vulnerability management program to record which vulnerabilities have been addressed.

> *An effective vulnerability management program should be integrated tightly with the patch and release management processes*

The patch management process should also be integrated with the change management process to ensure that software updates and releases are applied in a controlled manner. It is also important to ensure that the vulnerability management process scans systems post any updates to ensure the update has been applied properly and that it addresses the identified vulnerability.

Mobile Device Management

Mobile devices are now a pervasive part of the IT landscape, bringing unique security and management risk. Mobile devices evade traditional vulnerability and compliance management methods, and mixed ownership and control models (corporate-owned devices vs. BYOD) create policy gaps.

Integrating with Mobile Device Management (MDM) systems or deploying technology such as agents will enable organizations to add mobile devices to the assets identified and managed as part of the vulnerability management program.

Mitigation Management

An element often overlooked as part of an effective vulnerability management program is how to manage vulnerabilities in the event no software update or fix to address the vulnerability is available. There always will be a period of time from when a vulnerability is discovered until a permanent fix to address it is available from the vendor. As a result, an organization's assets will be exposed to compromise until the fix is available. An effective vulnerability management program will identify alternative ways to manage the exposure, such as changing firewall rules, increasing log monitoring, or updating IDS attack signatures, until the vendor provides a fix.

There always will be a period of time from when a vulnerability is discovered until a permanent fix to address it is available from the vendor

Incident Response

The security of an organization's systems is only as effective as how it responds to a security breach. The rapid response to a security incident can greatly reduce the impact the incident can have on the organization. However, many organizations view incident response as a function that should only be used in the event of a security breach. The modern threat landscape requires a more proactive approach to responding to known and potential incidents.

While the discovery of a critical vulnerability does not automatically mean a security breach has occurred, ensuring the incident response process is alerted to the issue can provide a number of benefits. First, it enables those responsible for incident response to be better prepared in the event an incident happens. It also allows the incident response team to ensure they have the appropriate tools and security monitoring in place in order to respond appropriately.

The discovery of a critical vulnerability does not automatically mean a security breach has occurred

During an incident, it may also be necessary to integrate the vulnerability management process so that systems can be scanned for potential vulnerabilities to either include or eliminate them as being potential points of compromise. In addition, the vulnerability management process can help the incident response team identify any other potential

vulnerabilities that attackers could leverage to compromise the systems.

Automation

The final key to a successful vulnerability management program is automation. Security solutions are often viewed as a means to stop or prevent a security breach. However, in reality this is often not the case. Depending on who or what is attacking the system, the various security solutions may simply be speed bumps and merely delay the attacker from reaching their goal. Therefore, time is of the utmost importance in detecting, assessing and remediating any vulnerability. Another motivation to automate where possible is the volume of data that may be required to be processed. This will depend on the size and complexity of the environment being managed; but many large networks constantly have devices being added, changed and removed constantly.

The manual processing of large amounts of data is extremely time consuming and prone to error. The final reason to automate is to reduce the human element from the process thereby reducing the risk of human error.

Key Performance Indicators to Improve Vulnerability Management

AN EFFECTIVE VULNERABILITY MANAGEMENT PROGRAM requires on-going care and attention. There is a famous management saying which states "you can't manage what you don't measure." This applies equally to running a vulnerability management program. In order to understand how effective the program is, or to identify areas that can be improved, it is important to have some Key Performance Indicators (KPIs) to highlight where the vulnerability management program is successful, where it is failing, and where efforts and resources need to be concentrated.

> *You can't manage what you don't measure*

Which KPIs are applicable to an organization can vary widely on a number of issues, such as the size of the organization, the industry it is

in, the type of systems it employs, and where its systems are located. Some common KPIs to measure are:

Number of vulnerabilities per vendor

This KPI can be useful in helping identify vendors that may not have a good track record in provide secure solutions. Should a vendor have a large amount of vulnerabilities it may indicate a quality control issue within their own development processes. This information can be useful when selecting new solutions from vendors as vendors with a history of having a large number of vulnerabilities, particularly if they are of a critical nature, may be rated as a higher risk than those with a lower number.

Number of vulnerabilities per product

This KPI can be a useful indicator as to where most vulnerabilities lie and on what types of products. This can be then used to allocate appropriate resources to enhance the security of that product. It can also be used in identifying more suitable alternatives to the affected products.

Aging of vulnerabilities

This KPI can be used to measure the effectiveness of the patching program. Ideally this KPI can be broken down further based on the criticality of the vulnerabilities. Knowing how long it typically takes to apply a patch to a vulnerability is a useful metric when determining an organization's exposure to a newly announced vulnerability and what steps to take to reduce that exposure

Percentage of systems scanned

Networks, by their nature, are volatile environments; systems and devices connect and disconnect from the network regularly. When a vulnerability scan is conducted, there is no guarantee that all devices will be scanned. Knowing the percentage of an organization's computer estate that has been scanned can help identify whether or not the scanning should happen more regularly, at different times, or if alternative and more effective means of scanning need to be employed.

Number of vulnerabilities over time

Monitoring the number of vulnerabilities over time is an important KPI. Ideally the number of vulnerabilities detected over time should trend downwards, indicating the vulnerability management program is working.

Summary

THE VOLATILITY OF TODAY'S THREAT LANDSCAPE, the growing complexity of the computer systems and networks within organizations, coupled with the speed of change means that effective vulnerability management is a critical element in securing those networks, systems, applications and data. Vulnerability management has to evolve beyond being simply an exercise scheduled to run a few times a year to becoming a continuous process proactively identifying potential issues.

Equally important is ensuring the vulnerability management process is integrated tightly with other processes and that these processes complement and enhance each other's capabilities. In particular, the ability to detect new assets on the network and to quickly scan them for vulnerabilities and threats is critical. Due to the volume of data to be processed automating the different processes and their interdependencies will be vital to maintain the security posture of the organization.

The ability to detect new assets on the network and to quickly scan them for vulnerabilities and threats is critical

An effective vulnerability management, integrated with other disciplines throughout the organizations, is fast becoming a necessity to ensure the security of their systems. It's no longer a question of "should a comprehensive vulnerability management be implemented?" Rather the question is "when will the comprehensive vulnerability management program be implemented?"

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.