happiest minds
The Mindful IT Company
Born Digital . Born Agile

VULNERABILITY MANAGEMENT

A HYBRID FRAMEWORK APPROACH

Vishwanath P.R

Yogesh B S

ABSTRACT

In this paper, we propagate the idea of a framework for vulnerability management to meet the Infrastructure security and compliance requirements standards of an organization.

Vulnerability management is the integral component of a security program which includes detection, assessments, remediation and tracking.

This white paper provides an overview of how to approach and manage a vulnerability in the infrastructure until remediation.

The importance of this study is to promote best practices on how to approach the different categories of vulnerability in the IT Infrastructure and ease the efforts of security professionals in implementing a good security program.

TABLE OF CONTENTS

INTRODUCTION

Vulnerability Management Program

Every organization needs a Vulnerability Management for its assets connected to the internet. Many industries are striving hard to be compliant with regulations. Most of the attacks which are resulted in data loss are often caused due to usage of known, unpatched vulnerabilities. Vulnerability Management comes handy for those assets on your network that is not regularly monitored for patches.

Vulnerability Management is fundamental to Computer Security and Network Security, which helps in identifying the vulnerability and takes necessary action whether to eliminate, mitigate or tolerate vulnerabilities based on its risk and cost. Vulnerability Management consists of several specific steps such as Discover, Classification, Assess, Reporting, Remediation and Verification. This is a continuous process that monitors closely and provides a feedback loop on the ongoing Network Threat Management.

Vulnerability Management is BAU (Business, As Usual)

Vulnerability management is a continuous process that ideally helps organizations better manage their Infrastructure vulnerabilities in the persistent future. A good Security program is constituted from a matured model implementation which is an ongoing process, and to protect organization and data, Vulnerability Management is recommended as the best practice.

The Center for Internet Security (CIS) Top "20 Critical Security Controls", like Basic CIS Controls, Foundational CIS Controls and Organizational CIS Controls. Implementing the CIS Top 20 critical security controls is a great way to secure and strength the Organization network.

An effective list of Critical Security Controls for an Organization security posture

Basic CIS Controls:

01 Inventory of Authorized and Unauthorized Devices

02 Inventory of Authorized and Unauthorized Software

03 Secure Configurations for Hardware and Software

04 Continuous Vulnerability Assessment and Remediation

05 Controlled Use of Administrative Privileges

06 Maintenance, Monitoring, and Analysis of Audit Logs

Foundational CIS Controls:

Email and Web Browser Protections	Malware Defenses	Limitation and Control of Network Ports
Data Recovery Capability	Secure Configurations for Network Devices	Boundary Defense
Data Protection	Controlled Access Based on the Need to Know	Wireless Access Control
Account Monitoring and Control		

Organizational CIS Controls:

Security Skills Assessment and Appropriate Training to Fill Gaps	Application Software Security	Incident Response and Management
Penetration Tests and Red Team Exercises		

VULNERABILITY MANAGEMENT LIFE CYCLE

Figure 1: Vulnerability Management Life Cycle

The steps in the Vulnerability Management Life Cycle are described below.

Discover

To discover assets in the organization, usage of automated tools which can help us identify IP based devices to keep an accurate account of assets. Need for discovery process is a must to ensure inclusion of all IP based devices. To do this, we need to prepare and keep track of hardware and software inventory, and to identify all IP's scanners should be able to scan the entire subnets or agent-based approach. It is crucial to review and configure discovery scan settings at each cycle. Finally, credential scan or authenticated scan reveal more information than just IP's such as software installed, databases, open ports, protocols, and services.

Classification

In this stage, we need to prioritize the assets by categorizing the business unit based on the criticality to business operation. The main goal is not to attend the low priority assets while keeping the high-impact assets vulnerable.

Assessment

The assessment stage includes identifying vulnerabilities through automated scans and credentialed scans. In order to run a vulnerability management program, we must continuously reiterate the configuration changes which provides breadth and depth of scanning range. Breadth is achieved by scanning every asset in the environment. Depth is achieved by providing credentials. Ensure the scanners are updated to the latest versions before running the scans, and all the non-intrusive checks are enabled. One of the main challenges in the authenticated scans is credentials supplied in the policy are not successful due to account lockouts, lack of permissions or ports such as 22, 139, and 445.

Note: All the scheduled scans are to be run in the window after the close of business, so that the network congestion does not impact the network bandwidth.

Report

In this stage, the report generated should reflect the audience. There are different types of reports, such as executive report, technical report, summary report, and remediation report. Knowing our audience, we can generate reports in a different format. The security professionals refer the technical reports, executive reports are generated for technical managers, and remediation report are generated for the patch management team.

The Information security team needs information about the success of scanning strategies to track remediation efforts.

Remediate

In this stage, the remediation efforts are tracked based on the plan of actions such as patches from vendors (OS or applications), configuration changes like registry changes, version update, or upgrade. Keep a rollback plan for any impact. When creating the plan of action's, one must keep in mind the order of preference like Prioritize and mitigate the vulnerabilities based on the business risk.

The number of counts the vulnerability exists in the infrastructure	Age of the vulnerability	Criticality of assets
Ease of exploitation	Severity of vulnerability	Zero days

Verify

Finally, to cross-check whether all the remediation efforts were successful or not initiating rescan with the same configuration ensures that no vulnerability are present in the environment. Tickets need to be closed after this step and keeping it as a reference for the future if any justifications required for accepted vulnerabilities such as no patch for zero-days, business justification for legacy applications, database or protocol in use should be documented.

VULNERABILITY MANAGEMENT PROCESS

Vulnerability Management is the process of identifying, evaluating, treating and reporting on security vulnerabilities in systems and software that runs on them. The Vulnerability Management Process Involves five phases.

Preparation

The first phase in Vulnerability Management is the preparation phase. Instead of considering thousands of vulnerabilities together, it is always recommended to start with a smaller number or by limiting the number of vulnerabilities identified by the vulnerability scanner.

The Information Security Team handles all the responsibility of this preparation phase in an organization. The very first step of the Vulnerability Management Process is defining its scope. Obtaining an agreement is very important and to analyze which system to be included or excluded from the Vulnerability Management Process. Besides the in-scope systems, an organization should also determine the type of scans. The Scan performed might be from the perspective of an external attacker on the external network or from the perspective of an internal attacker on the internal network.

Vulnerability scan

Once the preparation phase is complete, the next phase of the process begins, and the initial vulnerability scans are performed. Any issues which occur during the scans must be recorded as it might happen again in the future like unavailability or poor application response. By recording this information, it reduces the impact of future scans over the performance or stability of the target systems. Most of the vulnerability scanning tools offer a wide range of reporting options to visualize scan results, and it is necessary to use these tools to create numerous reports.

Management and Information Security team shows more involvement to know the risk organization is currently facing that includes the rate of vulnerabilities detected and its severity of the detected vulnerabilities. The owner of the assets wants to get an overview of vulnerabilities in the systems that they are responsible.

The IT department will want an overview (per technology) of technical information about detected vulnerabilities as well as recommendations for mitigation and improvement.

Define remediating actions

In the next phase, the asset owners, along with the Information Security team and the IT department, will define remediating actions. The Information Security Team provides the input on risk remediation by analyzing the vulnerabilities and identifying its associated risk.

After analyzing the vulnerabilities from a technical perspective, the IT department suggest on the availability of the patches or whether to harden the configuration needs. The IT team also recommends on the feasibility of the possible remediating action like whether they can avail the same support from the vendor after updating patches.

The Information Security Team should set clear deadlines on the remediating action implementation in order to ensure enough priority is given to remediation. Asset owners must have a timeline in their action plan when to implement these remediating actions, and the timeframe should be in line with the level of risk detected.

Implement Remediating actions

According to the agreed timeframe, remediating actions should be executed based on the plan. It is always recommended to record if any problems occur and the asset owner should define an alternative action based on recommendations by the Information Security Team and IT Department. Then these new remediating actions should be implemented, and the Information Security Team should track the status of remediating actions.

Rescan

Rescan must be scheduled to verify whether remediating actions have been successfully implemented. Like the initial scan even this scan will be performed using the same vulnerability scanning tools and identical configuration settings. This is a very important step to prevent inaccurate results due to configuration errors. Generally, for implementing remediating actions, rescan is scheduled after the deadline. Like the initial scan reports even for these the same types of reports are created.
The management and asset owners will be interested to know whether the remediating actions have been effectively implemented and whether any residual risk remains. The IT department will be interested in how effective the remediating actions have been implemented.

The security team will analyze the vulnerabilities throughout the vulnerability management process, determine the associated risks and provides input on risk remediation. Further, from a technical perspective, the team will analyze the vulnerabilities and provides information on the availability of patches or whether to harden the configuration. This ongoing process has resulted in eliminating most vulnerabilities that cybercriminals use to breach an organization.

KEY FEATURES OF THE VULNERABILITY MANAGEMENT SYSTEM

Your vulnerability management system should be able effectively identify existing security and software misconfigurations, high-risk software, web server misconfigurations, and other vulnerabilities in your network.

Features to evaluate in a vulnerability management program include:

Security configuration management

Detection of antivirus enablement, ensuring secured password policy, ensuring authorized administrative share access, updated antivirus definitions, enabling MS Windows Firewall, folder share permissions, browser configurations, checking elevation of user privileges, and more.

Web server hardening

Security hardening of web-facing servers is essential. Your vulnerability management program must be powerful enough to secure communications via SSL to prevent attacks gated via the server. This will help to prevent denial of service and brute-force attacks.

High-risk software audits

Keeping the EOL (End of Life) Software or Legacy Software within the business operation, which makes them extremely vulnerable to exploits. Upgrade the EOL software, decommission the legacy software and the application should be scanned and defined permission for use or blockade. This will help to prevent the creation of new vulnerabilities that can invite attacks.

Port audits

Your Vulnerability Management program must have the capacity of controlling the firewall ports to determine which applications require the firewall ports to be open or closed, especially on internet servers. In case if inactive ports are open, then it might lead to exploitation by injecting trojans or other malware.

Zero-day vulnerabilities mitigation

Zero-day vulnerabilities are barely exploited in the wild and do not come with patches. Vendors strive hard to release timely patches before proof of concept is implemented. In such cases, a vulnerability management program must help execute custom scripts in the form of tweaking registry key settings or disable legacy protocols.

Did you know the ransomware WannaCry, which wreaked havoc in 2017 to businesses worldwide, came with a simple fix for disabling the SMB (Server Messaging Block) V1 and closing port 445? A lack of awareness led to widespread ransomware attacks.

SECURITY VULNERABILITY LIFE CYCLE

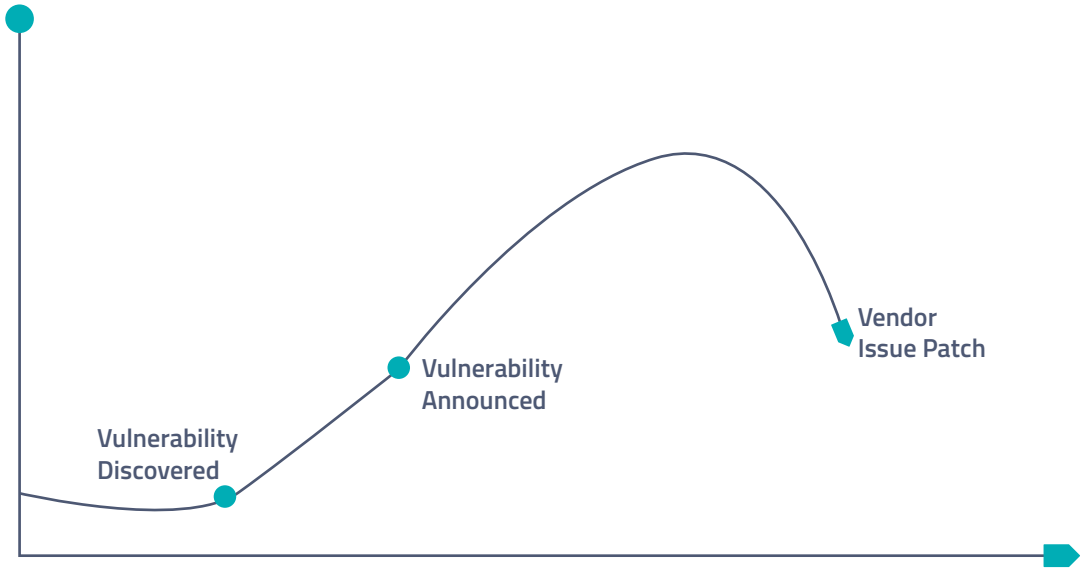

Figure 2: Security Vulnerability Life Cycle

There are four stages in the security vulnerability life cycle:

Vulnerability Discovered

This stage is when someone discovers a vulnerability.

Vulnerability Announced

This is when websites designed for announcing new vulnerabilities post a warning about the new hole discovered. At this stage, the attacker is also checking these websites to search for new exploits.

Vulnerability Popularized

In this stage, malware for this vulnerability is written and attackers would exploit them.

Patch Released

The final phase of vulnerability is when the vendor affected by the vulnerability releases a patch to protect against the attacks.

TRADITIONAL FRAMEWORK

Whenever a vulnerability is disclosed to the public through the CVE database, by the usage of automation tools like Nessus, Qualys Guard, Rapid7 Insight VM network scans are performed to discover, assess and report these vulnerability findings. When the vendor releases the patches for vulnerabilities, the patch management team use patching tools to deploy monthly patches, cumulative patches without the regard for impact analysis coverage. Without the proper process defined, it would be a tedious task to align or synchronize different teams to manage vulnerabilities with ever-growing CVE database. A lack of awareness of the impact of vulnerabilities among IT engineers leads to failure of such traditional frameworks.

With considerations of the cons of traditional frameworks, adopting a hybrid framework was much needed to implement a VM program.

How vulnerability management is an upgrade from legacy IT ops processes

Vulnerability management is an upgrade from the conventional IT management processes and provides an array of functionalities:

Inventory scanning

Taking inventory of the various software assets and creating custom groups based on OS and applications.

Vulnerability assessment:

Discovering all possible known vulnerabilities that can lead to attacks.

Vulnerability mitigation

Providing remedial advice to thwart the vulnerabilities.

Risk and threat prioritization

Defining the risks based on the severity and accordingly acting.

Most importantly for patch management, if patches are available for the known vulnerability, a built-in patch manager solution can resolve the vulnerabilities quickly.

PATCH MANAGEMENT

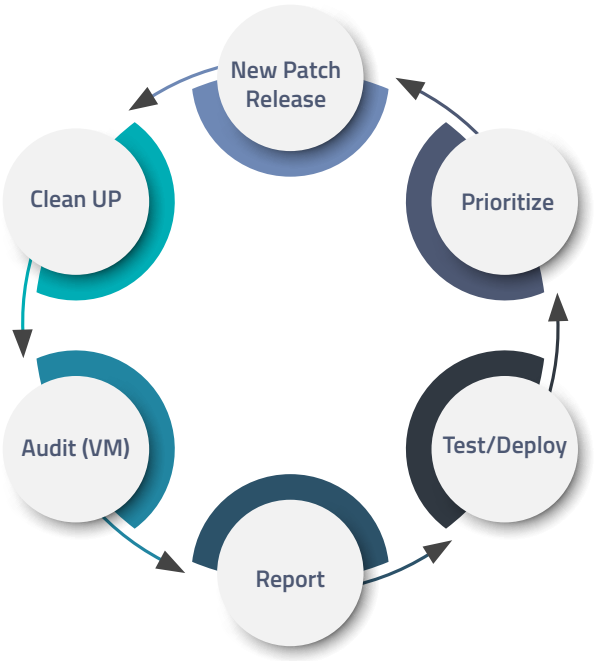

Figure 3: Patch Management

Patch management makes the process simple and easy to manage the patches and helps to acquire the patches, installing and then testing them. It helps to keep the system updated on all the security patches available. It also decides which patch should be used or which shouldn't be.

The software companies carry patch Management in order to detect any software bug and then release a patch for the same. A lot of difference has been seen since the inception of patches. Initially, the patches were sent over the external media devices and that too as individuals stand-alone code modules. It used to be based on traditional fee-licensing systems. But today in this digital era of web-delivered systems and cloud computing, the delivery system has undergone a sea change. Now patches are applied to programs over a global IP.

Eight easy steps that are used to implement Patch Management:

Security & Patch Information Sources

Automatic System Discovery

Prioritization and Scheduling

Testing

Change Management

Installation and Deployment

Audit & Assessment

Consistency and Compliance

Patching Approach do's and don'ts

DO: Adopt regular patching cadence, Chase remediations and utilize risk score.

Don't: Patch only when on fire, Chase Vuln Counts and Don't prioritize CVSS

It is important to generate granular reports once the vulnerabilities are discovered and remedied to help document for further purposes and security auditing. Enterprises need not have to worry about cyber threats if the right vulnerability management program is in place and hence focus on other areas of business.

DEMERITS OF TRADITIONAL APPROACH

With considerations of demerits of traditional frameworks, adapting a hybrid framework was much needed to implement an effective VM program. We can indicate some demerits with the traditional approach like complete removal of False Positive & False-Negative. False positive materializes when the scanner, Firewall or Intrusion prevention system quotes the vulnerability is present in the infrastructure whereas with False negative is the opposite, this quotes the vulnerability is not present in the infrastructure.

01 Does not update or maintain hardware and software asset inventory

02 All the vulnerabilities are approached in a similar type.

03 Do not comprise of specific skillset personnel in a team.

04 No residual cleans up.

05 Removal of old software's.

06 No monitoring of updates.

07 Impact analysis.

08 No synchronization among teams about the program.

With the above significant points in mind, we here propagate a hybrid approach with some of the modifications from the NIST framework and other research conducted in the universities.

HYBRID FRAMEWORK

Here in this hybrid framework, the demerits of the traditional approach have been converted into advantages. To introduces a new maturity model which has worked out in the current project. In this paper, we present to you some of the key modifications done and how we were able to solve some of the complex problems introduced in the Infrastructure vulnerability program. For example:

01 The reoccurrence of vulnerabilities – Supersede

02 The problem persists even after patch deployment.

03 Coverage of impact analysis.

04 Creating a baseline for reference to keep track.

05 Approach each category of vulnerabilities differently

By the time we write this paper, the framework built has matured into running this program smoothly. Security professionals can adopt this framework to make this better and seamless.

In the following section, we list the modifications introduced in the framework.

01 Data segregation based on the category.

02 Elimination of false positives, decommissioned assets.

03 Dividing each category of vulnerabilities to a team member.

04 Implementing registry changes

05 Clean-up procedure

06 Review of vulnerabilities by manual observation in the testbed environment.

07 Ensure impact analysis is covered in each stage patch test.

08 Design and maintain test plan.

09 Use of PowerShell Script to monitor version updates.

For Example: Here with the help of PowerShell script, we can identify the version upgrade/update is successful prior

```
$filename = "\Windows\system32\ntoskrnl.exe"
 $obj = New-Object System.Collections.ArrayList
 $computernames = Get-Content C:\Users\xyz\Desktop\Servername.txt
foreach ($computernames in $server)
{
$filepath = Test-Path "\\$server\c$\$filename"
 if ($filepath -eq "True") {
$file = Get-Item "\\$server\c$\$filename"
$obj += New-Object psObject -Property @{'Computer'=$server;'FileVersion'=$file.VersionInfo|Select
FileVersion;'LastAccessTime'=$file.LastWriteTime}
      }
   }

$obj | Out-Host

 select computer, FileVersion, lastaccesstime | Export-Csv -Path
'C:\Users\xyz\Desktop\File_Results.csv'
```

Categories of Vulnerabilities

Actions	Zero Day	OS Patch	Application Patches	Application Patches
Remediate	Need Immediate Patch by vendor	Need to plan organizational requirement accordingly (Month, Quarterly and Half yearly patch)	Update/Upgrade the Application Versions	Registry changes after patch deployment
Deployment	Implement workaround, if no patch from the vendor	Deploy patch, 2nd Tuesday of the month (Microsoft patch release)	Need to update the application patches every 15days	Reboot after fix
Testing time window	Low	Moderate/High	Low	Moderate
Complexity	Critical	Critical/High	Medium/High	Medium

Figure 3: Patch Management

CONCLUSION

Here we conclude by stating that the framework propagated is a continuous and on-going process which needs correction and execution in the Organization. The work and study conducted predominately over the windows environment.

By adopting these framework security professionals need to modify based on their Organization's requirements and business risk. Since different organizations have different needs and requirements, one needs to establish the importance of security policies as per organizational requirements and implement them accordingly.

AUTHOR BIO

Yogesh Babu B S *has over 12 years of experience in IT Industry as Server Administrator, VMware and Information Security. He is currently a part of the Infrastructure Management and Security Services Business unit in Happiest minds Technologies Ltd. He is responsible for Security Vulnerability Management, Vulnerability Assessment Project, SCCM, Servers, Microsoft Exchange and emerging technologies.*

Vishwanath P R *has over ten years of holistic experience in the field of Information Security. He is currently a part of the Infrastructure Management and Security Services Business unit in Happiest minds Technologies Ltd. He is responsible for Web Application Security, Infrastructure Vulnerability Assessment, Penetration Testing, and Vulnerability Management.*