Remediation Requirements
Vulnerability Management Plan

Prepared for

by Sean Cooper, on behalf of

Table of Contents

TABLE OF CONTENTS 2

REVISION CONTROL LOG 3

INTRODUCTION 4

SCOPE 4
LIMITATIONS 4
REFERENCES 4

VULNERABILITY MANAGEMENT PROCESS 5

STEP 1 – IMPLEMENTATION OF VMP & ACQUISITION OF RESOURCES 5
ACQUISITIONS ITEMS AND RESOURCES 5
STEP 2 – INFRASTRUCTURE SCANNING / INFORMATION GATHERING 6
STEP 3 – REMEDIATION PLANNING 6
STEP 4 – REMEDIATION EXECUTION 6
STEP 5 – VERIFICATION OF VULNERABILITY REMEDIATION / RESCAN 7

VULNERABILITY MANAGEMENT PLAN GUIDANCE 7

VULNERABILITY SCAN CYCLES 7
AUTOMATED NETWORK SCAN AND PATCH, EXAMPLE A – WEEKLY CYCLE 8
VULNERABILITY REMEDIATION CYCLES 8

REFERENCES 9

ACRONYMS AND ABBREVIATIONS 10

VENDOR DOCUMENTATION 11

SIGNATORY PAGE 12

Revision Control Log

Date	Old Version #	New Version #	Revised By:	Description
Oct 6, 2014	0.0	0.1	Sean Cooper	Initial Document Composition
	0.1	1.0	Sean Cooper	Final Document Delivery

Introduction

A vulnerability management plan is a set of policies, processes, procedures and assets that provides situational awareness of software vulnerabilities. Faithfully executed, a vulnerability management plan (VMP) enhances your computer security, allowing you to focus on generating profit for your business.

This documents purpose is to advise the client on the general costs and benefits of a VMP, as well as technical and procedural requirements to successfully implement the VMP.

A VMP is a required aspect of your organizations IT functions, as it addresses known and exploitable weaknesses in your company's defenses, many of which can be exploited to impact you with costly downtime and lost profits.

Scope

A VMP includes scanning for vulnerabilities, risk analysis of those vulnerabilities, remediation planning, patching, and re-scanning to make sure that the vulnerabilities have been closed.

Generalized guidance and best practices for the installation, configuration, operation and maintenance of specific IT systems is included in this plan.

Limitations

This plan is limited in its scope, in that it doesn't cover the day-to-day operation of the vulnerability management process or systems, such as the vulnerability scanner or the patch management system. Management of those specific systems is the responsibility of the Information Security Officer or designee.

This plan also does not cover the day-to-day management of use-specific appliances such as network routers, firewalls, storage devices or similar task-specific devices. Management of those specific systems is the responsibility of the Information Security Officer or designee.

References

For additional information on the subject, a "References" section has been added to this document, containing a list of other documents which provide guidance and template processes and procedures for this document.

Vulnerability Management Process

Vulnerability management is a process that encompasses the evaluation, analysis and remediation of vulnerabilities in an IT system. Using standardized methods to obtain a list of vulnerabilities, correct the vulnerabilities, mitigate the risk, or accept the risk, allows for situational awareness of the enterprise security posture. (SANS Institute, 2013)

The generalized process outline consists of 5 steps:

1. Implementation of VMP & Acquisition of Resources
2. Infrastructure Scanning / Information Gathering
3. Remediation Planning
4. Remediation Execution
5. Verification of Vulnerability Remediation / Rescan

These steps, followed in the numerical order listed, are the "heavy lifting" of implementing a VMP and are critical steps in securing an enterprise against malicious exploitation of software defects.

Step 1 – Implementation of VMP & Acquisition of Resources

The first step in a vulnerability management plan is designing the actual plan and receiving a formal policy endorsement. This plan can easily be adopted into your governance documentation by signing the Signatory Page of the document and disseminating it to the appropriate individuals for action.

Acquisitions Items and Resources

Technical Requirements		Manpower Requirements	
Item #	**Description**	**Item #**	**Description**
1	Dedicated VM or physical host for hosting of Vulnerability Scanning Software (VSS).	1	Approximately 20 man-hours / week for VMP execution.
2	Network accessibility from Item 1 to all machines that are targeted items for the VMP.	2	Approximately 5 man-hours / week for audit and assurance of VMP execution. This must be a separate person from Manpower Requirement 1.
3	Fresh, patched installation with A/V, A/M software. No other software installed.	3	Appropriate manpower (1-2 hours, monthly) to keep the dedicated scanning host properly patched and up-to-date.
4	Yearly or Perpetual license for NESSUS Vulnerability Scanning Software.		
5	Login credentials on the Microsoft Windows Active Directory Controller that provide administrative privileges as necessary for the VSS to operate.		
6	Login credentials on the Microsoft Windows Active Directory Controller that provide non-administrative privileges for the audit activities of the VMP.		

qWhen these items have been acquired and guaranteed by senior management, step 2 may be began.

Step 2 – Infrastructure Scanning / Information Gathering

Step 2 consists of two parts: identification of systems that will be a part of the vulnerability scanning, and the actual scanning process.

As a matter of policy, any computer (desktop, laptop, netbook, mobile, server, appliance or embedded) should be subject to regular vulnerability scanning and the vulnerability management process. Allowances may be given for production issues (the host was not on or accessible when the scan was performed), but the host must be scanned before being brought back online and put onto the production network.

Apprehension that the host may not "respond well" to scanning is not sufficient reason to avoid the scanning. The scanning is typically a very passive process, with load on the scanned system being low to moderate. A thorough testing cycle with the VSS and a representative test computer may be performed in an isolated environment if significant concerns are raised about the performance of a production host during the scanning cycle.

The actual scanning process is fairly automated. With a few clicks, a security personnel or designee can begin the scanning process using the login credentials provided on the dedicated VSS host. Specific documentation, with accompanying screenshots, can be found in the Nessus documentation or the {REDACTED} {REDACTED} Network Scanning Quick-Start Guide, included in the "Vendor Documentation" section of this document.

The deliverable for Step 2 of the VMP is a soft-copy of the vulnerability report, delivered to the overseeing security designee as well as the person who will be doing the remediation.

Step 3 – Remediation Planning

Remediation planning starts with an analysis of the delivered scan results, typically in a soft-copy format. This will indicate the nature of the vulnerability, if any exist, and the manner in which remedy for the software flaw can be applied. Remedy for the software flaw typically involves either a software package update (colloquially known as a "bug fix" or "patch") or a machine configuration update (with or without accompanying software package update).

Planning continues by identifying the necessary patches or configuration items to be applied, the manner in which they're going to be applied, and the timeframe in which they will be applied. The timeframe is generally subjective and based on business need for the systems in question. The CVE database, available at https://cve.mitre.org., is available for supplemental information on specific vulnerabilities. One of those supplemental information fields is an impact and urgency assessment which may be useful to your organization for planning the timeline and resource allocation of your organizations resources. It is HIGHLY recommended that any CRITICAL or HIGH vulnerabilities be fixed within 72 hours, as these are the most severe of the vulnerabilities and offer the most potential for attack and compromise of your systems.

When all necessary patches have a schedule installation order and date, and this has been communicated to the personnel who will be performing the remediation execution, step 3 may be began.

Step 4 – Remediation Execution

Remediation execution is, simply put, following the remediation plan document that was derived from the vulnerability report generated in Steps 1 & 2, respectively.

Remediation must have a testing phase in which remediation testing machines (machines that have similar configurations to production-level machines but are not required for normal business processes) have the

patch set applied to them, before being applied enterprise-wide, in which the functionality of the applications affected are verified. Only after the remediations have been tested, can they be applied to other systems in the enterprise.

This remediation can be achieved through automatic means, depending on the needs and capabilities of the organization. For some, the remediation execution might mean physically visiting each workstation, directing it to the appropriate software update resource and manually confirming the execution of the remediation activities. For others, the remediation activity might consist of configuring a Group Policy Object on the Microsoft Windows Active Directory Domain Controller to apply the appropriate configurations and patches, typically through Windows Software Update Service (WSUS) or a similar utility. Specific details on which process to follow will be a part of your IT departments Standard Operating Procedures (SOP) guide and are beyond the scope of this document.

For a Linux environment, remediation might be as simple as running a command line that checks a local package repository for newer versions of the afflicted (or, all) packages. An example would be:

```
#yum update
```

Devices such as switches, routers, firewalls, NAS/SAN devices and other purpose-specific devices can be updated, usually by obtaining updated software/firmware from the vendor, and then applying the updated package in the manner suggested by the vendor. Specific details on which process to follow will be a part of your IT departments Standard Operating Procedures (SOP) guide and are beyond the scope of this document.

Allowances may be given for production issues (the host was not on or accessible when the remediation was performed), but the host must be fully remediated before being brought back online and put onto the production network, or it would represent a large surface for attack

Step 5 – Verification of Vulnerability Remediation / Rescan

Audit and verification of remediation activities should be performed on a “spot-check” basis on several of the representative machines.

The audit activities consist of another full scan of the machines subject to recent remediation activity to ensure that all of the critical/high remediation activities were successful. Additionally, it is suggested that all the moderate and low remediation be performed, as well. If time or resources do not permit full remediation of all vulnerabilities, the critical ones must be addressed first, high vulnerabilities next, and moderate/low vulnerabilities last.

Vulnerability Management Plan Guidance

Vulnerability Scan Cycles

Vulnerability scans should be run once every business week, to provide ongoing situational awareness of the security posture of the enterprise. If possible, these scans should be run daily to provide maximum benefit and to accelerate the remediation cycle. These scans can be automated and performed during off-hours to lessen or eliminate impact on end-users.

The scans should utilize all possible plugins provided by Nessus, to allow for maximum detection of outdated or misconfigured software. A custom scan policy can be engineered and provided, if desired.

If a highly-automated system is desired, it is suggested that the Nessus scan be configured to run before, and then again after, the Windows Update and all vendor updates. If the Nessus scan is configured to output a report automatically at the end of its scan, most of the "heavy lifting" will be done automatically, in that the initial survey scan will be completed, the patch cycle will be completed, and then the verification / audit rescan will be completed without human intervention. Information security personnel would still need to certify that the targets are correct and represent the entirety of the enterprise, verify the audit report and spot-check the installation of the patches.

Automated Network Scan and Patch, Example A – Weekly Cycle

	SUN	MON	TUE	WED	THU	FRI	SAT
Nessus Scan – Survey	X						
Vulnerability Review		**X**					
VRP Drafted			X				
VRP Tested				X			
VRP Approved					X		
VRP Scheduled					X		
VRP Executed						X	
Nessus Scan - Audit						X	
VRP Results Audited							**X**

X = Manual Steps, X = Potentially Automated Steps, X = Short Steps

Vulnerability Remediation Cycles

The vulnerability remediation cycle is dependent on the frequency of the scan cycle, with an added overhead of the time it takes to perform the remediation planning and execution. For example: if the scan cycle is performed on Sunday morning, and the time to formulate and approve the remediation plan, do the required testing of the remediation plan, and approve the remediation plan is 4 business days, the remediation cycle is once every five days.

While the best remediation cycle is immediate and continuous, that approach is not practical for an organization that doesn't have dedicated IT staff on hand. For organizations such as that, it is suggested that the remediation cycle be approximately 1 week in length and 1 week apart, yielding 2 scan/remediate/audit cycles per month. The most time that should elapse between scans is 25 business days with 5 days of planning and execution time, yielding 1 scan every calendar month.

At the end of every remediation cycle, a report should be prepared and delivered to the CTO or other security or compliance designee, containing the following:

- Number of Vulnerabilities Found, Number of Vulnerabilities Remediated
- Supporting Evidence (i.e., Nesus Scan Reports, before and after remediation)
- Number of Platforms with Remaining Flaws, Percentage of Platforms with Remaining Flaws
- Estimated / Rounded Number of Hours Spent in Remediation Activities
- Estimated / Rounded Number of Hours Required to Remediate Remaining Vulnerabilities

References

Mccully, G. (2013, June 17). *Components of an Effective Vulnerability Management Program - SecureState*. Retrieved from SecureState Blog: http://blog.securestate.com/components-of-an-effective-vulnerability-management-program/

National Institute of Standards and Technology. (2013, July). *GUIDE TO ENTERPRISE PATCH MANAGEMENT TECHNOLOGIES.* Retrieved from NIST Special Publication 800-40, Revision 3: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

SANS Institute. (2013, 03 23). *SANS Institue - Implementing a Vulnerability Managment Process.* Retrieved from SANS Institute: http://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180

Acronyms and Abbreviations

Abbreviation or Acronym	Meaning
VMP	Vulnerability Management Plan
CTO	Chief Technology Officer
CSO	Chief Security Officer
VSS	Vulnerability Scanning Software|System
NAS	Network-Attached Storage
SAN	Storage-Attached Network
SOP	Standard Operating Procedure|Process
IT	Information Technology
WSUS	Windows Software Update Service
CVE	Common Vulnerability and Exposure
VRP	Vulnerability Remediation Plan

Vendor Documentation

Title	Description	Document
Guide To Enterprise Patch Management Technologies	NIST Special Publication 800-40 on Patch Management in an Enterprise IT Environment	NIST.SP.800-40r3.pdf
Implementing A Vulnerability Managment Process	SANS Institute Guide on Implementing a Vulnerability Management Process	SANS Institute - Implementing a Vulr
{REDACTED} {REDACTED} – Network Scanning Quick-Start Guide	Customized documentation describing the procedure for initiating and exporting a Nessus vulnerability scan on the dedicated VSS host.	To Be Delivered
Nessus Installation Guide	A guide for the installation and configuration of the Nessus product.	nessus_5.2_installation_guide.pdf
Nessus User Guide	A guide for the use and maintenance of the Nessus product	nessus_5.2_enterprise_user_guide.pdf
Common Vulnerabilities and Exposures	A list of shared vulnerabilities and configurations that are known to provide attack vectors into vulnerable systems.	http://cve.mitre.org/

Signatory Page

I/we, the undersigned, accept this document, titled "Vulnerability Management Plan" into our corporate IT policies and procedures, this day, the ____ of _____, _____.

We agree to faithfully execute this Vulnerability Management Plan to the best of our abilities according to the procedural and notional guidance contained herein. We indicate and affirm that this document shall be the controlling document with respect to vulnerability assessment and management within our organization.

We agree to provide funding for both the initial acquisitions listed, as well as maintenance funding to keep those tools up to date and properly licensed.

_____	_____
Signature Date	Signature Date
_____	_____
Printed Name Title / Position	Printed Name Title/Position
_____	_____
Signature Date	Signature Date
_____	_____
Printed Name Title / Position	Printed Name Title/Position