GUIDE

Best Practices Guide: Vulnerability Management

A Straightforward Guide to Successful Vulnerability Management for Infrastructure and Applications

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction

If you are new to vulnerability management or looking to refresh your knowledge, the information in this guide should help you to quickly understand the choices you have available. You will read advanced-level content created by IT Security engineers with hands-on experience in IT security and vulnerability management. By the end of this document you should understand the benefits of vulnerability management and be confident about the next steps to make your organization's IT infrastructure and applications more secure.

Enjoy!

Chapter 1: Introduction to Vulnerability Management

What is the Cause of IT Security Vulnerabilities?

Making information exchange available to customers and business partners, by definition, requires that companies have a connection to the outside world. Keeping the information secure from attackers becomes the challenge. There is a consistent stream of new security vulnerability discoveries due to flaws in software development, improper configuration of hardware and software applications, and the inevitable unintended errors made by IT users. Your business can be susceptible to hackers and criminals if IT security vulnerabilities are not identified and fixed on a regular basis.

Vulnerabilities generally fall into three categories: vendor, system, and user-originated. Vendor-originated vulnerabilities are programming mistakes in software that include insecure services or non-robust implementations of protocol standards. System-originated vulnerabilities include improper configuration of applications and lack of password protection policies. User-originated vulnerabilities result from falling prey to malware (Ie. Phishing emails), and not running anti-virus software.

It is important to identify the primary threat vectors your organization must worry about. Attackers will attempt to exploit any given vulnerability in the following ways:

- Outsider attack from networks (wired and wireless), web application, telephone (PBX or VOIP)
- Insider attack from local network, local system, malware

A serious concern is that once a single vulnerability from outside the organization is compromised, that system can be used as a springboard for additional attacks on the same network.

What is Vulnerability Management?

Vulnerability management is the ongoing practice of detecting, classifying, prioritizing, and remediating security vulnerabilities in IT infrastructure and applications. Vulnerability management requires an automated process to efficiently address exploitable security holes as well as a documented security policy that is adhered to in order to drive compliance. The methods used to address vulnerability management can vary, but the primary goal remains the same… reduce overall risk to corporate and customer data.

How Has Vulnerability Management Evolved?

IT security vulnerabilities have been prevalent since the dawn of computer systems. You may be familiar with viruses and malware, but there are underlying vulnerabilities in systems and software that hackers and cyber-criminals seek to exploit. These attackers can target specific confidential information, trade secrets and even personal identities. Historically, companies used one-time penetration tests as an approach to evaluate IT security by simulating an attack on computer systems, networks, or applications from external and internal threats.

More recently, vulnerability scanners have augmented penetration testing using software to uncover vulnerabilities in networks and systems in a more automated fashion. The term vulnerability management is often confused with vulnerability scanning. Vulnerability management is the process surrounding vulnerability scanning, also taking into account other aspects such as risk acceptance and remediation. Vulnerability management is as much a people process as a technology process.

Why is Vulnerability Management Important?

In some industries certain types of data and how the data is handled securely is strictly regulated. Regulators commonly require a documented security process, and vulnerability management results can serve that purpose. Moreover, effective vulnerability management can be a business advantage by providing insights for decision-making, reducing the time and resources required for compliance, and safeguarding your company's reputation. Vulnerability management, and the practice of reducing information security risk, can complement and enable your business objectives.

Chapter 2: The Vulnerability Management Process

Vulnerability Detection and Discovery

The first step in the vulnerability management process is identifying your IT assets and discovering vulnerabilities. This typically involves directing a vulnerability scanner at a range of IP addresses or, in the case of a web application, a specific web address (URL). The vulnerability scan will inventory hardware, software applications, services and configurations. Vulnerability scanners will identify holes in your systems and networks from both an internal and external perspective. It can also identify rogue systems and devices that are connected to the network without authorization.

Before launching a vulnerability scan you need to have your organization's IP ranges for domains and sub-networks. You also should alert the appropriate individuals in your organization so that scanning does not create false alarms or create disruption in the production environment.

What to Scan?

You will want the vulnerability scan to be comprehensive. Everything that is connected to your company's network should be scanned in a broad range of categories including:

- Servers – Operating Systems, Web Servers, Email Servers, etc.
- Databases
- Firewalls
- Switches and hubs
- Wireless Access Points
- Client devices (where applicable)
- PBX and VOIP systems

Vulnerability Classification and Prioritization

Not all vulnerabilities are created equal. The Common Vulnerability Scoring System (CVSS) and Common Vulnerabilities and Exposures (CVE) are government and industry efforts for communicating the characteristics and impacts of IT vulnerabilities.

Vulnerability scanners categorize and rank vulnerabilities based on technical and business risks. The objective is to identify the issues that could impact the most critical systems or data, so you know what to fix first. The generally held categorization includes: Critical, High, Moderate/Medium, and Low. The severity level indicates the security risk of the vulnerability and the difficult of exploiting the vulnerability. The theory is that the more severe the vulnerability rating, the more at risk your organization is to attack. If there is a known exploit, the likelihood of an attack is much higher. In other cases, it often depends on both the technical risk as well as the business importance of the asset on which the vulnerability resides.

Vulnerability Remediation

Fixing security issues and reducing your company's risk of a security breach is the core of vulnerability management. You should prioritize remediation of the most critical issues as quickly as possible. As stated earlier, vulnerability management is as much a people process as a technology process. This is the point at which vulnerability identification transforms into vulnerability management.

Most vulnerability scanners and vulnerability management solutions will provide guidance on remediation with a focus on how to mitigate risks. They also have a built in ticketing system, or the ability to export vulnerability issues to an external tool. This can help expedite remediation as it can facilitate cross-team collaboration on fixes. For example, if a critical vulnerability is found in a web application, a support ticket can be created and assigned to a developer on the web team.

Reporting

Reports are used to document the data found during the previous phases of vulnerability management and provides a view appropriate for different audiences. Different reports are generally made available from templates targeting the specific audience. Some reports are targeted for auditors and industry regulators. Others formats help confirm compliance with internal operating policies. It is common for the technical report to include a threat level from low to critical, vulnerability rating, analysis of the issue, and the impact on the information asset in the event that the vulnerability is exploited. An executive summary will recap the overall risk posture and describe general findings.

Common components in a vulnerability management report include:

- Assets covered in the detection phase
- Graphs and/or charts depicting overall risk status
- Prioritized listing of vulnerabilities ranked by risk rating
- Trending of vulnerabilities from discovery and remediation perspectives
- Trouble-ticket status
- Technical information about unremediated vulnerabilities

A vulnerability report would not be complete without documented recommendations to secure any high-risk systems and detailed technical information on how to mitigate the vulnerabilities. You should be able to understand the tasks needed to resolve the issues and how much effort may be required to implement the recommended fix.

Chapter 3: Vulnerability Management Recommendations

How Should You Prepare for Vulnerability Management?

You should have an objective for implementing a vulnerability management solution. Vulnerability management is a commitment to decreasing the risk of a security breach and ensuring compliance with your company security policies. It is an assurance to your company, your partners and your customers.

You need to gain the support and commitment to vulnerability management from company leadership, since this undertaking will require diligence and participation of employees across all areas of the business.

Depending on how you choose to implement a vulnerability management solution, it may require IT staff to assist with deployment. It is vital that everyday operations of your

organization will not be disrupted in the implementation of your vulnerability management solution. Remember that vulnerability management is an ongoing effort; so ensure that your time and resources are budgeted appropriately.

What Determines the Cost of Vulnerability Management?

The truthful answer to this question is, it depends. There are multiple options for how you can implement a vulnerability management solution including hiring a consultant, running the software yourself, or even outsourcing the duties to a managed service provider.

Open Source software can be an inexpensive option up front, but you need to be prepared for the costs to deploy and administer the solution. Your security team must have the knowledge to operate the tools. And you need to be prepared for limited training and technical support.

Commercial software and Software-as-a-Service (SaaS) vary from relatively inexpensive to prices that requires budget, process, and purchase orders. Commercial software can cost the same to run as Open Source, whereas SaaS places the burden of hardware infrastructure and technical support on the vendor.

Vulnerability management vendors have different pricing models. In most cases, the cost is directly related to the size, complexity and the number assets being checked for vulnerabilities. One of the major advantages of vulnerability management is that once a solution is in place, the process of detecting, prioritizing, and remediating vulnerabilities is virtually on-demand and the incremental costs are negligible.

How Should You Select a Vulnerability Management Provider?

Your choice needs to incorporate your budget and resource considerations. Because you are protecting your organization's most valuable assets from security breaches, you will want to select a vendor that balances a solid track record of performance with cutting-edge security innovations.

You should seek out a provider that understands the unique needs of your IT environment and has the flexibility to deliver a customized solution. With efficient and effective remediation being the end goal, having a provider that integrates well with your existing security and management tools should be a strong consideration.

You should consider asking the vulnerability management provider for a list of references from organizations with a similar profile to yours. You may also ask the vendor for examples of similar projects they have undertaken in the past. There are common accreditations in the IT security industry and you can ask to confirm the credentials and experience of the individuals who will oversee the vulnerability management services for your company.

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com