Cybersecurity Tech Basics: Vulnerability Management: Overview

SEAN ATKINSON, CIS™ (CENTER FOR INTERNET SECURITY), WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

A Practice Note providing an overview of what cyber vulnerability management programs are, how they work, and the key role they play in any organization's information security program. This Note discusses common types of cyber vulnerabilities and core process steps for implementing and maintaining a vulnerability management program to decrease cybersecurity risks. It also addresses common pitfalls that can lead to unnecessary cyber incidents and data breaches.

Most organizations depend on a combination of commercial and custom-developed hardware and software products to support their information technology (IT) needs. These technology components inevitably include vulnerabilities in their design, setup, or the code that runs them. Cyber vulnerabilities, coupled with growing threats, create risks by leaving organizations open to attacks, data breaches, and other cyber incidents. These events often lead to regulatory enforcement, litigation, or credibility loss. Organizations and their counsel must understand these risks and address vulnerability management in a well-defined and managed information security program.

This Note provides an overview of what cyber vulnerability management programs are, how they work, and the important role they play in any organization's information security program.

VULNERABILITY MANAGEMENT DEFINED

Vulnerabilities are weaknesses or other conditions in an organization that a threat actor, such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to adversely affect data security. Cyber vulnerabilities typically include a subset of those weaknesses and focus on issues in the IT software, hardware, and systems an organization uses. For example:

- Design, implementation, or other vendor oversights that create defects in commercial IT products (see Hardware and Software Defects).
- Poor setup, mismanagement, or other issues in the way an organization installs and maintains its IT hardware and software components (see Unsecured Configurations).

Vulnerability management programs address these issues. Other common vulnerabilities that organizations must also tackle in their information security programs include:

- Gaps in business processes.
- Human weaknesses, such as lack of user training and awareness.
- Poorly designed access controls or other safeguards.
- Physical and environmental issues.

Unlike threats, organizations can often directly control their vulnerabilities and therefore minimize the opportunities for threat actors.

Organizations that develop their own in-house software should use security by design techniques to avoid creating vulnerabilities. For more information on assessing overall data security risks and related legal considerations, see Practice Note, Data Security Risk Assessments and Reporting (W-002-2323) and Performing Data Security Risk Assessments Checklist (W-002-7540).

Vulnerability management programs:

- Define a formal process to:
  - timely identify applicable vulnerabilities;
  - close the security gaps that vulnerabilities create by remediating or at least mitigating their effects; and
  - track and document an organization's efforts.
- Prioritize often limited IT resources. Organizations must focus on vulnerabilities according to their level of risk, particularly considering the sheer volume of changes that diligent vulnerability management can demand.
- Continuously monitor and evaluate an organization's IT environment to ensure compliance and avoid re-introduction of known vulnerabilities.

- Minimize cyber attack risks by decreasing the number of gaps that attackers can exploit, also known as the organization's "attack surface."

Some refer to vulnerability management programs as "patch management" because vendors often provide software patches or updates that organizations can apply to remediate their systems. However, applying patches is only one means of managing some vulnerabilities. Organizations can also protect themselves by using secure configurations and defense-in-depth techniques that layer multiple security controls. Sound vulnerability management programs take a broad view and leverage patching and other safeguards.

Vulnerability management programs play an important role in any organization's overall information security program by minimizing the attack surface, but they are just one component. For details on the key steps for implementing a formal vulnerability management program, see How Vulnerability Management Programs Work. For information on building a comprehensive information security program, see Information Security Toolkit (W-002-8679).

HARDWARE AND SOFTWARE DEFECTS

Defective hardware and software products are the source of many cyber vulnerabilities. Vendors fail to follow security by design principles or fully test their products. The tactics, techniques, and procedures (TTPs) that attackers use have grown increasingly sophisticated. Changing TTPs mean that some vendors' designs may not have contemplated certain attack strategies. Attackers also range from unskilled amateurs, known as script kiddies, that use other hackers' tools to malicious insiders, activists, criminals, and highly funded nation-state actors. For more information on common cyber attacks, see Practice Note, Cybersecurity Tech Basics: Hacking and Network Intrusions: Overview (W-003-3498).

This heightened threat climate results in a larger number of identified vulnerabilities. Vendors typically identify hardware and software product vulnerabilities using several methods, including:

- **Testing.** Vendors perform their own product testing, and in some cases, employ internal or external security specialists that focus on discovering and fixing vulnerabilities. These specialists are usually called white hats, red teams, ethical hackers, or in the case of external experts, penetration testers. Building in strong security measures or fixing identified vulnerabilities often competes with other business priorities. This conflict and the complexity of full security testing for many products, especially given attackers' changing TTPs, results in distributed products that still contain vulnerabilities.
- **Active exploits.** Vendors may learn of product vulnerabilities only after attackers exploit them and victims, law enforcement, or other incident responders identify them as the attack's cause. These unfortunate situations are called "zero-day vulnerabilities." Vendors generally have time to provide a fix for identified vulnerabilities before attackers exploit them. Here that is not the case, hence the zero-day term. Some actors, including governments, allegedly identify and hoard vulnerabilities, using them to attack others rather than timely notifying vendors.
- **Bug bounty and vulnerability disclosure programs.** Formal vulnerability disclosure programs and policies set boundaries for security researchers, commit organizations to avoid legal action if others follow their policies, and provide guidance on how to notify them of identified vulnerabilities. Some organizations provide cash or other incentives to encourage good-faith responsible security researchers. The incentives are typically known as "bug bounty" programs. Several specialist companies offer bug bounty program management and support services and are well-known in the security researcher community.

Following vulnerability identification, vendors generally provide a software patch or other fix using an advisory. Hardware defects can be more challenging to remedy in current products, although vendors may provide software fixes or information on mitigation techniques. Industrial control systems and the increasing use of internet of things (IoT) devices present additional opportunities for hardware defects. These products can be:

- More vulnerability-prone due to manufacturers' too frequent lack of security focus and expertise.
- More difficult to remediate because of their limited user interfaces and lack of update capabilities.

For more information on gathering vendor advisories, see Maintaining Awareness and Detecting Vulnerabilities.

UNSECURED CONFIGURATIONS

Improper configurations or poor system management can cause cyber vulnerabilities even in fully patched hardware and software components. Factory-default settings may include easily guessed passwords or leave unnecessary services running.

Each organization's IT environment and business needs are unique. Reviewing typical device and software categories allows an organization to recognize and avoid potential vulnerabilities, by considering, for example:

- **Network elements.** Various network elements, such as routers, switches, and firewalls, provide internal and external connectivity and control network traffic. Organizations configure these devices with rules to distinguish potentially malicious traffic from legitimate data flows. Incorrectly applied rules, misconfigured access controls, or unnecessarily open hardware and software entry points or "ports" can:
  - create unnecessary vulnerabilities; and
  - make the organization vulnerable to network intrusions and data theft or exfiltration.
- **Servers.** Organizations often maintain their own servers for various IT functions, including end user file sharing and printer support, databases, applications, and websites. General purpose servers commonly run Windows, Linux, or Unix operating systems and by default enable a wide variety of services and communication mechanisms. Organizations should tailor these default settings to a server's particular purpose and their specific needs to reduce the attack surface. Servers also often have factory-default administrative settings and passwords that may leave the organization vulnerable to attack unless changed.
- **End user devices.** Attackers increasingly target end user devices, such as desktops, laptops, and mobile devices, because they provide an entry point into an organization's broader IT environment (for more details on these attacks against end users,

see Practice Note, Cybersecurity Tech Basics: Malware and End User Attacks: Overview (W-003-4711)). Vulnerabilities commonly occur when organizations fail to securely configure and maintain the devices with:

- current anti-virus and other tools to counter malicious software (malware);
- host-based firewalls to protect them from unauthorized internet traffic; and
- data encryption of personal information or other confidential data.

- **Browsers.** Web browsers typically include configuration settings for code execution and digital certificate handling. Mismanaging these settings creates vulnerabilities by potentially allowing unauthorized programs to run or users to access malicious, unsecured, or otherwise unreliable websites.
- **Other software and applications.** Commercial software and applications often similarly include default configuration settings that organizations must tailor to avoid vulnerabilities, such as:
  - allowing for unauthorized code execution; and
  - creating unprotected internet communication channels.

Organizations should maintain an accurate asset inventory and establish secure configuration standards for each major device and software category to avoid creating unnecessary vulnerabilities. For more on these process steps, see Maintaining an Asset Inventory and Establishing Secure Configurations.

HOW VULNERABILITY MANAGEMENT PROGRAMS WORK

Vulnerability management requires an ongoing, cyclical process because:

- New vulnerabilities are regularly identified and made public.
- Previously identified vulnerabilities can still create cyber attack opportunities, if organizations:
  - do not promptly remediate them; or
  - allow their re-introduction through poorly configured or mismanaged devices and systems (see Unsecured Configurations).

Five core process steps help organizations implement and maintain a reasonable vulnerability management program. Specifically, organizations must:

- Understand their current IT environments by tracking hardware and software assets, including current versions and applied patches (see Maintaining an Asset Inventory).
- Set standards for the hardware and software components that they use to avoid creating unnecessary vulnerabilities (see Establishing Secure Configurations).
- Stay abreast of newly identified vulnerabilities in the hardware and software products that they use or plan to use (see Maintaining Awareness and Detecting Vulnerabilities).
- Remediate or at least mitigate the effects of identified vulnerabilities according to the risk and exposure levels that they create (see Mitigating and Remediating Identified Vulnerabilities).
- Continuously monitor their IT environments to identify vulnerable assets and avoid re-introduction of known vulnerabilities (see Continuously Monitoring the Organization's IT Environment).

MAINTAINING AN ASSET INVENTORY

Organizations cannot protect assets unless they know about them. Maintaining a detailed IT hardware and software asset inventory, including specific versions, is a foundational element of any best practices based information security program (see Best Practices).

Tracking IT assets at an enterprise level can be complex and challenging because:

- Organizations constantly add, remove, and change their IT assets.
- Virtual server environments that run multiple systems or functions on a single hardware platform often include various software packages and versions.
- Organizations typically allow at least some individuals to install software on the laptops or other end user devices that they use, creating significant variation and more software packages to track.
- Bring Your Own Device (BYOD) programs that allow employees to connect their own mobile devices to an organization's network and systems, while convenient and cost-effective, often require organizations to manage additional software packages. For more information on BYOD programs and a sample policy, see Standard Document, Bring Your Own Device to Work (BYOD) Policy (1-521-3920).
- Increased use of cloud computing environments may require unique management processes, according to the particular deployment models chosen.

Some organizations integrate automated IT asset tracking systems into their procurement, deployment, and maintenance processes. These tools can help track larger and more complex environments, but can be costly to implement and maintain. Other organizations use ticketing systems, custom-developed databases, or even manual processes and spreadsheets to maintain inventory lists.

Regardless of the method or tools chosen, reasonably controlling vulnerabilities requires organizations to:

- Diligently maintain their IT asset inventories.
- Assign authority and establish information security policies to ensure that they acquire, develop, and track IT assets in a secure manner.

For more details on developing information security policies and a model policy, see Practice Note, Developing Information Security Policies (W-001-1336) and Standard Document, Information Security Policy (W-001-2990).

ESTABLISHING SECURE CONFIGURATIONS

Organizations often create unnecessary cyber vulnerabilities by deploying IT hardware and software components with default settings or unnecessary services (see Unsecured Configurations). Defining standard secure configurations for the organization's preferred network elements, servers, and end user devices helps manage vulnerabilities by:

- Creating deployment checklists, templates, or system images that take the guess work out of ensuring secure deployments.
- Avoiding activation of unnecessary services or other security gaps by tailoring setup to the organization's particular needs and environment.
- Minimizing the number of variations, especially in large organizations that may have hundreds or thousands of each device type.

- Simplifying patch management when vendors provide fixes for hardware and software defects (see Hardware and Software Defects).
- Providing a known baseline that organizations can deviate from when special needs arise by documenting exceptions in the organization's asset inventory (see Maintaining an Asset Inventory).

For resources and guidance on establishing secure configurations, see Best Practices.

MAINTAINING AWARENESS AND DETECTING VULNERABILITIES

Organizations must maintain constant awareness and diligence to stay abreast of newly identified vulnerabilities in the hardware and software products that they use or plan to use. Specific individuals should be accountable for monitoring various resources, such as:

- Applicable vendor security advisory email lists and blogs, including technically detailed versions for IT professionals. Many vendors provide security-related information on their websites at [company].com/security.
- Government agency email lists and blogs that aggregate vendor reports and provide public security advisory notices in some countries. Examples include:
  - US Computer Emergency Readiness Team (US-CERT) bulletins on their National Cyber Awareness System and the National Institute of Standards (NIST) National Vulnerability Database;
  - UK National Cyber Security Centre threat alerts and advisories;
  - South Korea's KrCERT security bulletins (in Korean); and
  - Canadian Cyber Incident Response Centre (CCIRC) bulletins.
- Cyber information sharing groups, such as industry and sector-specific information sharing and analysis centers (ISACs). Some ISACs focus on particular geographies, while others serve common critical infrastructure sectors, such as financial services.

The sheer volume of advisories can be overwhelming for some organizations, especially those that use a variety of hardware and software products. Organizations should:

- Determine exposure levels for each specific vulnerability by reviewing published risk ratings and their own IT environment's characteristics.
- Set remediation priorities according to risk and exposure levels. For example, a low risk advisory that applies to one or two internally facing servers likely does not require the same level of urgency as a high risk advisory that affects all laptops and desktops.

For resources on understanding typical risk ratings and other information often found in advisories, see Best Practices.

MITIGATING AND REMEDIATING IDENTIFIED VULNERABILITIES

Organizations typically remediate identified vulnerabilities by:

- Applying patches or other vendor-supplied updates for hardware and software defects (see Hardware and Software Defects).
- Updating configurations to use more secure settings or deactivate unnecessary services or communication channels (see Unsecured Configurations).

Some organizations use automated software distribution tools or other products to apply patches and track software updates, especially those with large or complex IT environments. Smaller organizations with simple environments that consistent mainly of end user devices may depend on vendors' automatic update features, such as Microsoft's Windows Update.

Some systems cannot tolerate patching because:

- Testing for internally or custom-developed software fails.
- Different vendor product combinations create incompatibilities.

Organizations may require additional time to patch systems that run highly available business critical operations. Patches may not be available for older legacy systems that organizations still depend on for important business functions.

Mitigation techniques or compensating controls help manage risks on these systems. For example, an organization may isolate vulnerable systems on dedicated network segments or apply additional access, auditing, or monitoring controls.

Organizations with more complex environments, especially those with internally or custom-developed software, generally test patches and other remediation measures in dedicated testing environments before deployment. Software patches can have unintended effects, so remediation plans should include system restoral options. Organizations should integrate their vulnerability mitigation and remediation activities into existing IT change management procedures to avoid inadvertent business impact.

Mitigation and remediation activities are not complete until they update the organization's asset inventory to document changes made and software installed (see Maintaining an Asset Inventory).

CONTINUOUSLY MONITORING THE ORGANIZATION'S IT ENVIRONMENT

Sound vulnerability management requires ongoing vigilance to identify vulnerable assets in an organization's IT environment and avoid re-introduction of known vulnerabilities, because:

- Over time, system configurations change, sometimes weakening security controls and creating inadvertent gaps.
- New installs or changes to an organization's IT environment may leave specific network elements, servers, laptops, or other devices unprotected from known vulnerabilities. For example, some updates may inadvertently remove previously applied patches or change secure settings.

Organizations ideally scan and assess their environments on a continuous basis, especially higher risk or more exposed elements. Regularly scheduled assessments demonstrate diligence and help minimize gaps. Various commercial and open source tools provide these monitoring capabilities. The security content automation protocol (SCAP) and related specifications define a set of standards for vulnerability scanners. Organizations use these tools to scan their environments and identify:

- Devices that have not been patched to remediate known hardware and software defects (see Hardware and Software Defects).
- Systems with unsecured configurations settings or other security gaps (see Unsecured Configurations).

NIST's SCAP Validation Program accredits independent laboratories which in turn test and validate vendor products against the SCAP standards. NIST maintains a list of currently validated products.

AVOIDING COMMON PITFALLS

Organizations still battle the same cybersecurity issues identified more than 15 years ago, particularly in supporting proactive vulnerability management and continuous monitoring. Several common pitfalls hamper many organizations' efforts to manage cyber vulnerabilities, including:

- Lack of a current well-maintained hardware and software asset inventory.
- Failure to routinely monitor vendor and other reliable sources for vulnerability advisories.
- Failure to prioritize vulnerabilities according to the exposure and risk levels they create for the organization.
- Lack of resources or willingness to timely remediate or mitigate known vulnerabilities.
- Use of outdated hardware, software, and legacy systems that cannot tolerate patching.
- Lack of standards for common device and system configurations, complicating patching and other remediation efforts.
- Failure to test patches before deployment or align vulnerability management activities with IT change management processes, leading to inadvertent business impacts or other unintended consequences.
- Failure to continuously monitor the organization's IT environment to identify vulnerable components and avoid re-introducing known vulnerabilities.

Organizations can avert these issues by:

- Establishing leadership support.
- Allocating sufficient resources.
- Following well-established best practices.
- Conducting periodic audits and program reviews.

For more resources on building strong information security programs and avoiding common pitfalls, see Information Security Toolkit (W-002-8679).

BEST PRACTICES

Vulnerability management programs have long been a part of reasonable information security programs. Best practices and other resources are widely available to help organizations build robust programs, including:

- The NIST Cybersecurity Framework, which is a risk-based methodology for building a comprehensive information security program, including vulnerability management (for more details on the Framework, see Practice Note, The NIST Cybersecurity Framework (5-599-6825)).
- The CIS™ (Center for Internet Security) Critical Security Controls, which provide an informative reference for the NIST Framework and detail 20 key information security controls, including:
  - Control #1: inventory and control of hardware assets;
  - Control #2: inventory and control of software assets;
  - Control #3: continuous vulnerability management;
  - Control #5: secure configuration for hardware and software on mobile devices, laptops, workstations, and servers;
  - Control #9: limitation and control of network ports, protocols, and services; and
  - Control #11: secure configuration for network devices, such as firewalls, routers, and switches.
- Detailed guidance on secure configurations for common devices and systems, which are available from most vendors and independent sources, such as:
  - NIST's Common Configuration Enumeration (CCE) resources; and
  - the Center for Internet Security's CIS Benchmarks™.
- The Common Vulnerability Scoring System (CVSS), which defines a standardized approach for describing and scoring vulnerabilities, according to risk and severity levels.
- The Common Vulnerabilities and Exposures (CVE) list, which provides an internationally recognized standard for naming and cataloging known cybersecurity vulnerabilities, with a maintained list of many publicly released advisories.

Organizations should:

- Garner leadership support and resources by emphasizing the preventive nature of vulnerability management programs.
- Cleary communicate the urgency and importance of remediating vulnerabilities across the organization. Promptly remediating vulnerabilities can prevent many data breaches and cyber incidents.
- Use established methods to score identified vulnerabilities according to their risk and exposure levels and accordingly prioritize their remediation plans.
- Document their vulnerability management activities, including the time required to patch or otherwise remediate issues. Program documentation allows organizations to:
  - continuously improve their programs; and
  - demonstrate their diligence if a data breach or other cyber incident occurs and regulatory enforcement action or litigation ensues.
- Perform regular program audits to ensure they are addressing vulnerabilities in a timely manner and according to risk and exposure levels.
- Treat their vulnerability management process as one element of a comprehensive information security program that is actionable, repeatable, and measurable.

07-18