How to Develop an Effective Vulnerability Management Process

Mark Nicolett

IT organizations should develop vulnerability management processes that protect IT environments against external attack and internal threats, and ensure corporate compliance with government regulations.
WHAT YOU NEED TO KNOW

IT security organizations should implement a vulnerability management process that includes a vulnerability assessment and security configuration baseline. Mitigation activity should be prioritized based on the severity of the vulnerability, the current threat environment and the business use of the vulnerable asset. Shielding should be used to protect vulnerable assets until mitigation is completed. The root cause of vulnerabilities should be identified and eliminated through improvements in network, server and PC configuration policies, and better change management and administrative processes.

ANALYSIS

A major responsibility of IT security organizations is to define and operationalize security policies that protect the IT environment from external and internal threats, and also provide compliance with regulations. Effective protection of IT resources requires a combination of approaches that include:

- Vulnerability management
- Shielding at the network and system layers
- Network access control (see "Protect Your Resources With a Network Access Control Process")

Vulnerability management is an ongoing process that establishes and maintains security policies for network and system resources; discovers, prioritizes and mitigates vulnerabilities; and eliminates their root causes (see Figure 1).

Figure 1. Vulnerability Management Process

Source: Gartner Research (February 2005)
The vulnerability management process consists of seven steps:

**Step 1: Policy**

The first step to improve IT security is defining the desired states for network and system configurations, resource protection and resource access. This requires the creation of policies that define secure configurations for network devices, servers, personal computers and other IT components; administrative constructs for users and application resources; and administrative processes that implement the policies.

**Step 2: Discovery and Baseline**

The next step is discovery of the network, system, desktop and data components that comprise the IT infrastructure, followed by the establishment of a security baseline. The discovery and baseline step must encompass systems that are corporate-owned and managed, and corporate-owned and unmanaged, as well as external systems and applications that access the corporate network.

*Vulnerability Assessment:* Vulnerability assessment provides a "bottom-up" baseline of the environment with respect to a database of known vulnerabilities. IT security organizations require a network-based approach that does not require management agents and can discover and evaluate vulnerabilities in managed and unmanaged systems. Many vulnerabilities are the result of configuration issues. Elimination of configuration-oriented vulnerabilities and their root causes requires a second baseline perspective — compliance with security configuration standards.

*Security Configuration Policy Compliance:* Security configuration policy compliance (SCPC) provides a "top-down" baseline of the environment with respect to security configuration policies that are organization-specific but are derived from industry-recognized best practices — such as the Microsoft Security Guide, the SANS (SysAdmin, Audit, Network, Security) Institute, the Center for Internet Security, the National Institute of Standards and Technology or the National Security Agency — vendor-defined interpretations of regulatory requirements, or corporate-defined configuration standards. The SCPC baseline audits the environment and discovers deviations from an organization's security configuration policies.

An SCPC baseline is well-suited to the work of vulnerability remediation. The initial steps of configuration policy development force the collaboration of IT security and IT operations, and ultimately lead to the elimination of the root cause of configuration- or administration-based vulnerabilities. Policy definition and periodic audits are also important components of an organization's regulatory compliance program. Standard configurations are a prerequisite for automated-provisioning processes, and support higher levels of availability and reduced operations costs.

*Convergence of Vulnerability Assessment and Security Configuration Management:* IT security groups that have attempted to use the output of a vulnerability assessment baseline to drive vulnerability mitigation projects within IT operations have found the data disorganized and unusable. As a result, reporting and analysis require the integration of vulnerability assessment and security configuration management data. IT security organizations should pressure vendors for analysis that cross-references vulnerabilities and configuration changes.

**Step 3: Prioritization**

When organizations baseline their environments in regard to vulnerabilities or security configuration standards, they need to do more mitigation work than time and resources will permit. Therefore, mitigation efforts need to be prioritized according to these factors:
The Nature of the Vulnerability and the State of the Current Threat Environment: As cyberattackers become more efficient at quickly exploiting software vulnerabilities, IT security managers need current information about the external threat environment. Vulnerability management products must factor near-real-time threat information into vulnerability prioritization and alert functions.

The Business Use of the Vulnerable Asset — Asset Inventory and Classification: Asset inventory and classification is a prerequisite for the second aspect of prioritization, which is the business use of the vulnerable asset. In general, vulnerabilities that are likely to be attacked and are present on business critical assets that are not effectively shielded should have the highest mitigation priority, but there are exceptions. When a vulnerability is widespread and subject to a worm attack, it needs to be mitigated — regardless of asset use. On the other hand, if a vulnerability exposes corporate data or applications to inappropriate internal or external access, the business use of the asset becomes a major determinant of mitigation priority.

The classification of assets by business use is required by both IT security and IT operations. IT security uses asset classification for business-oriented risk analysis, vulnerability mitigation prioritization and the generation of security metrics. IT operations uses asset classification in the areas of business-relevant availability, capacity, change analysis and reporting on service-level agreements. Asset classification requires a substantial amount of initial project work. Ongoing maintenance requires well-developed processes across the IT organization. The majority of vulnerability assessment, security management and operational configuration management tools build and maintain system inventory data in product-specific repositories. Organizations should establish a single source for asset classification so that maintenance costs are minimized. This strategy requires that systems and security management products support the import and export of asset classification and business service data.

Step 4: Shielding and Mitigation

Mitigation is the slowest, most-difficult part of vulnerability management because it requires the management of changes that are implemented across many IT operations and support areas. The IT security group is responsible for developing security administration and configuration policies, and must monitor the current state of the environment with respect to those policies; however, the network, server and desktop support organizations carry out the bulk of the mitigation work. Rapid patching alone is an inadequate response to vulnerability mitigation (see "IT Operations Must Change to Deal With Windows Attacks"). Use technologies such as firewalls, network- and host-based intrusion prevention, and network access controls to shield vulnerable assets until mitigation work has been completed.

Workflow: Workflow functions are needed to organize mitigation work. There is a requirement for loose integration with operational workflow processes. There is also a requirement for embedded workflow within vulnerability management products for organizations that have not yet deployed enterprise workflow systems, and to address situations where detailed vulnerability information is too sensitive to expose within the enterprise workflow system.

Automated Mitigation: Automated mitigation of vulnerabilities is possible but not commonly deployed on a wide scale. For example, it is possible to completely automate the download and installation of security patches but a completely automated approach is only common for consumer PCs. In a corporate environment, patch installation occurs only after quality assurance testing is completed, and is scheduled within a time widow that is appropriate for the applications or business functions supported by the system. We see the same situation for other types of system changes that are related to vulnerability management. In most cases, it is useful to have the vulnerability management baseline generate the system change, and stage the change so that it can be implemented at the appropriate time in the context of a change-management process. More-aggressive forms of automation are appropriate in a small number of cases.
Examples include scan and quarantine at network connect time and the automated elimination of some configuration errors or unwanted functions on corporate PCs.

**Vulnerability Management and Network Access Control (NAC):** There is widespread demand for the capability to evaluate the security state of systems as they connect to the network, implement a network access policy and mitigate discovered vulnerabilities. Incumbent vulnerability assessment or security configuration management tools can potentially provide NAC baseline and mitigation functions in specific customer environments (see "Protect Your Resources With a Network Access Control Process").

**Step 5: Controls/Eliminating Root Cause**

As organizations take action to eliminate the vulnerabilities that have been exposed by the security baseline, they also need to evaluate the overall pattern of vulnerabilities to identify and eliminate the root causes. Many vulnerabilities are the result of poorly formed system configuration or user administration policies, and inadequate provisioning or change management processes. Eliminating root causes requires improvements in the policies and processes that are used to provision, configure and change systems, and administer users.

**Step 6: Maintenance**

IT operations is responsible for the bulk of vulnerability remediation project work, the implementation of virtually all system maintenance and administrative changes, and the provisioning of new systems and users. An effective vulnerability management program requires that security configuration and administration policies become part of day-to-day operational tasks (see "IT Security and Operational Management Must Converge").

**Step 7: Monitoring**

New attacks can emerge and spread rapidly, and new applications and administrative changes can introduce new vulnerabilities. The activities of system users and system administrators must also be monitored. The discovery and baseline steps need to be continuous, and all subsequent vulnerability management steps should be repeated as part of an ongoing process. Up-to-date vulnerability assessment and security configuration information is needed:

- To monitor the security state of the IT environment and the current status of patch management and vulnerability mitigation activities
- To discover unmanaged and misconfigured devices as they connect to the network
- As an input to IT security risk reporting
- As a data feed to the real-time event prioritization functions of IT security management systems

IT security management technologies can also be used to monitor external threats to the IT environment and to provide additional information about specific changes that have caused lapses in security configuration or security administration policies.

**Technology Evolution**

Vulnerability assessment and security configuration policy compliance tools have been used by IT security organizations for discovery and baseline for many years. However, major changes in tool deployment and data use are driving changes in the vulnerability management market. Vulnerability assessment and security configuration management are evolving from utility functions that periodically generate reports for security personnel to security infrastructure that provides near-continuous scanning and reporting for IT security and operations. Integration and
cross-referencing of vulnerability assessment data with security configuration policy compliance data is needed to improve data use for mitigation. Improvements in asset classification and risk analysis will enable security reporting and metrics for IT and business area management.

Key Issues

How will enterprises manage IT configurations to eliminate vulnerabilities and implement security policies?

This research is part of a set of related research pieces. See "Improve IT Security with Vulnerability Management" for an overview.