

Security Demands Drive Shift to Vulnerability Management

Enterprises that practice sound vulnerability management, rather than only intrusion detection, will experience fewer cyberattacks and suffer less damage from them.

Core Topic

Security and Privacy: Security Management Strategies and Processes

Key Issue

How will enterprises manage the complexity of authentication and access control in a highly distributed world?

Strategic Planning Assumptions

Through 2006, 75 percent of system and application changes, excluding user administration, will be driven by security demands (0.8 probability).

By year-end 2005, the due diligence level of vulnerability assessment will require that full system scans be done at least once per month (0.7 probability).

The most effective — and cost-effective — way to ensure enterprise security is to only install secure software products that are configured according to security policies. However, most software is not secure enough to meet rapidly evolving threats. Therefore, enterprises must take the second-best approach: find and mitigate vulnerabilities, and shield vulnerable assets. Sound vulnerability management practices will reduce the number of successful attacks and the overall cost of security.

Prediction — Enterprises that implement a vulnerability management process will experience 90 percent fewer successful attacks than those that make an equal investment only in intrusion detection systems.

During the past year, most organizations have learned that perimeter firewalls, antivirus software and intrusion detection systems are not enough to protect them from cyberattack. Attacks have moved to the application level, circumventing network-based firewalls. Worms propagate so quickly that signature-based antivirus protection is useless. Intrusion detection systems do not provide protection, only faster notification that your security has failed.

The ideal form of protection requires hardened, locked-down server and desktop configurations with near-real-time patch deployment. However, most corporate systems are not, and will never be, locked down or hardened. Therefore, a layered approach is required that shields vulnerable systems from attack during the vulnerability mitigation process.

Vulnerability management is a set of processes and technologies that are used to:

- Establish and maintain a security configuration baseline

Gartner

- Discover, prioritize and mitigate vulnerabilities
- Establish security controls
- Eliminate root causes

Vulnerability management requires functional interfaces between the IT security organization and other support areas, such as desktop support, server administration and network support.

Strategic Planning Assumption: Through 2006, 75 percent of system and application changes, excluding user administration, will be driven by security demands (0.8 probability).

Action Recommendations for 2004

Establish a working group composed of security, desktop support, server administration and network support personnel. This group should develop and deploy joint processes and technology selection criteria to cover configuration management and vulnerability mitigation. You will not find an integrated set of products that spans everything from vulnerability assessment to patch management to intrusion prevention. Rather, selectively deploy products that solve discrete sets of operational and security issues. An example of this type of integration can be found in products that integrate patch analysis with packaging and software distribution to automate patch management. In many other cases, you will need to select standards or middleware that allows the integration of best-of-breed security products with best-of-breed configuration, network and systems management products.

Prediction — Near-continuous vulnerability assessment scanning will replace periodic scans that are based on an audit schedule.

Scanning products traditionally have been run only to prepare for a periodic external audit or as part of external consultancies that conduct yearly penetration tests. This approach is useful for security audits, and sometimes useful for making a case internally that more security oversight is needed to control network and system administrators. However, infrequent vulnerability scans do little to make the environment more secure.

Near-continuous scanning is needed to quickly identify new vulnerabilities because application, network and system changes invariably introduce configuration errors, and new vulnerabilities frequently are announced by system and application vendors. Because cyberattackers are continually scanning for openings, enterprises need to find these vulnerabilities before the attackers do. They then must take two key actions:

- Some form of temporary shielding must be installed between the vulnerability and potential attackers.
- Vulnerabilities must be prioritized and passed to a mitigation process that involves the network, server, application and desktop support areas.

Strategic Planning Assumption: By year-end 2005, the due diligence level of vulnerability assessment will require that full system scans be done at least once per month (0.7 probability).

Action Recommendations for 2004

Scanning products must become part of the security infrastructure and should:

- Provide near-continuous scanning
- Generate alerts when a system change creates vulnerability
- Identify "unmanaged" nodes on the corporate network
- Receive frequent updates from external threat monitoring services
- Provide a standards-based interface to firewall, antivirus and intrusion prevention systems to support rapid shielding

Bottom Line: Security demands will drive a new focus on highly proactive vulnerability management. Near-continuous scanning will rapidly become a standard enterprise requirement as security administrators struggle to stay ahead of vulnerabilities that are introduced by software vendors, as well as configuration errors committed by internal personnel. Although vulnerability management is a labor-intensive solution to a fast-growing problem, it is the most-realistic way for enterprises to protect their systems.