

# Risk Management Vulnerability Management

Vulnerability management encompasses a number of related disciplines, some of which are processes in and of their own right. The intent of a vulnerability management program is to ensure that current security issues within the environment are identified, evaluated using a risk management approach, and dealt with in a cost-effective and efficient manner.

## **SOLUTION**

A vulnerability management program typically incorporates the following elements:

**Risk Management Strategy** – The overall program should be based on a risk management approach, which is used to guide decisions and evaluations dependent upon the associated level of risk to the organization, rather than blindly trying to deploy all patches as they come out, or making decisions “in a vacuum.”

**IT Management and Practices** – Although it’s not enough to apply general IT best practices such as change management, cross-training, documented procedures, system monitoring, and disaster recovery planning, these types of activities are vital to ensuring the ongoing security and availability of an IT environment in the long term.

**Patch Management** – Making sure relevant patches are applied in a timely manner ensures continued functionality and availability of services, as well as protecting against malicious

software and other attackers. However, the current ongoing deluge of patches for virtually all operating systems, devices, and platforms requires a disciplined approach in order to identify those patches that are relevant, ensure consistent application across affected or exposed systems, and optimize system availability.

The previously described elements of a vulnerability management program (Risk Management, IT Management and Practices), work together in supporting and providing for an effective patch management effort. Patching efforts should be guided by prioritization of important patches and the potential impact of not patching. Infrastructure should be in place to allow new patches to be identified, tracked, and assessed for risk and importance, in addition to being deployed and confirmed.

**Anti-Virus Program** – An effective and comprehensive anti-virus program that protects both permanently connected and transitory elements of the overall environment is a must in the current age of fast moving and widespread viruses, worms, and Trojans.

This requires a strong process to ensure adequate coverage is in place and that deployed anti-virus products are kept up to date. This typically requires assigned responsibilities for monitoring virus alerts, procedures for deploying both regular and emergency updates, and a means to confirm that updates have been successfully distributed and systems are up to date.

**Self Testing for Vulnerabilities** – Periodic self-checks for issues using vulnerability assessment tools are an important quality assurance activity to ensure that the overall vulnerability management program is effective. It also serves to confirm that system configurations are appropriate and not exposing unnecessary services or holes, and allows administrators to correct problems proactively.

#### **SUMMARY**

All of these program elements require resources – staff resources and time to conduct the necessary activities, processes to define what is to be

done, management support to ensure the necessary follow-through, and infrastructure to enable the activities to be done efficiently. Many of these elements have a reputation for being complex and cumbersome, but they generally do not have to be.

Despite the overhead, even lightweight versions of these processes are critical to the efficient operation of an IT environment. They are even more vital for smaller IT shops, where traditionally these activities have been only casually followed due to resource shortages. It can be argued that such resource shortages make the use of a vulnerability management program a necessity, in order to ensure time and effort are carefully managed and prioritized to achieve the maximum benefit for the organization.

Documenting at least the core elements of the information involved and changes made is especially important to an environment where the loss or unavailability of even a single team member can be a major issue, or where additional resources must be quickly brought up to speed.