



Fact or Fiction: Debunking the Top 5 Misconceptions about Vulnerability Management

Wednesday, March 26, 2008

www.lumension.com



Overview

Vulnerability management can be a powerful means toward reducing the threat surface within an enterprise IT environment. But because vulnerability management technology has been around in some form or another for so long there has been plenty of time for the din of marketing-speak from various vendors to confuse users about the true nature of vulnerability management tools and practices.

The following are some of today's most common myths perceived about vulnerability management, along with explanations for why these beliefs are false. Understanding the true nature of vulnerability management will allow organizations to better mitigate risk and to ultimately strengthen the synergy between IT security and operations.

Fiction:

All vulnerability management systems are created equally.

The Facts:

One of the biggest myths held by those purchasing security solutions is that all vulnerability systems are alike. However, there are many details in each that can affect performance and, ultimately, usefulness of the system.

When evaluating a system it is critical to look at the source of vulnerability definitions used to assess the environment, how well the system integrates with the IT infrastructure and how actionable the information is that is produced by the system. Ideally a system should link vulnerabilities to as many standard vulnerability classifications as possible, such as CVE, BugTraq and IAVA codes. And most importantly, it should be integrated within the architecture to be able to automate and report on remediation to the greatest extent possible. Unfortunately, many vulnerability management systems on the market today fail to include this key element of automated remediation, making it an arduous task to actually fix the vulnerabilities found during assessment.



Fiction:

Patching is the only way to remediate vulnerabilities.

The Facts:

Even non-security experts understand that many of the vulnerabilities within an organization's infrastructure come by way of bugs and coding problems in their vendors' software. As a result patch management rightfully gets a lot of attention as a powerful means to remediate vulnerabilities.

But patch management is only half of the vulnerability management picture. The other half is configuration and change management. According to both Forrester Research and Gartner analysis, more than 40 percent of application downtime is caused by configuration problems. Vulnerability management best practices call for both up-to-date patches and flawless configurations to mitigate risks that can cause downtime or potential data breaches.

Sound configuration management tools and processes will not only address certain vulnerabilities left untouched by patching, they can also be a way to reduce risk when a patch cannot be administered. For example, take a certain little-used process that is always on by default. If that process is found to be flawed but the patch to fix it causes some other unrelated but vital process to break, it might make sense to change the default and turn that process off rather than installing the patch. For this reason the best vulnerability management tools will marry both patch management and configuration management in a single package.

Fiction:

Agent-less solutions are better than agent-based.

The Facts:

Over the years the debate over vulnerability management system agents on the endpoint has raged, spurred on primarily by rhetoric from vendors who only offer one choice of assessment method.

Those in the agent camp say an agent is a best way to enforce patch and configuration levels on a consistent and ongoing basis. Those for agentless systems believe that network scanning can offer a better view of a dynamic network environment, examining and discovering new machines



that may not have agents and other vulnerabilities that might not be found with an agent. The truth of the matter is that both sides are right—both agents and network scanning offer their own intrinsic strengths. So why should an organization have to choose between these methods?

A truly thorough vulnerability management system should be able to offer both agent and agentless assessment and remediation capabilities. Without both methods, an organization is bound to leave a gaping hole within their vulnerability management activities.

In the case of solely relying on agents, an organization can potentially be blindsided by devices and laptops without agents installed that connect to the network. Working only with an agentless system leaves the possibility open that a device or laptop may not always be connected during a scan, thereby falling through the cracks. Taking advantage of both techniques takes advantage of each side's strengths while eliminating their weaknesses.

Fiction:

Vulnerability management technology will always give you a big-picture view of risk.

The Facts:

Because all vulnerability management tools are not created equally, many of them can fail to offer their purchaser a fully fleshed view of the risk suffered due to vulnerabilities.

Many tools that are evolved from the old guard of what was once the vulnerability assessment market are often guilty of producing long and detailed vulnerability reports that tend to offer a myopic look at the flaws in an environment. These reports are often not correlated to the configuration controls in place within the network environment. This makes it difficult to comprehensively mitigate risk through change and configuration management without the vulnerability system indiscriminately throwing up a red flag because a patch has not been installed.

Additionally these laundry list reports offer little in the way of actionable or prioritized information. They are meant to be produced by the security team, which then typically lobs the reports over to an already beleaguered operations team to handle the problems in a 'firefighting' mode. Without that integration of automated remediation these tools make it difficult to not only evaluate and prioritize risks posed by vulnerabilities, but to also act upon that information.



Fiction:

Installing vulnerability management system solves all of your vulnerability problems.

The Facts:

A good vulnerability management system can provide the make-or-break difference for a successful security program. But it is not a panacea. Risk cannot be solved, it can only be mitigated. And because vulnerabilities and the threat surface changes every day, that risk is a moving target. Which means that vulnerability management systems at their very core are not install-and-forget tools.

In order to maximize the power of a solid vulnerability management system, an organization must set the right policies and procedures in place. Ideally the organization should get a picture of the current landscape and the risks posed by known vulnerabilities and then set a configuration baseline that mitigates the risks deemed most important to that enterprise based on threat relevance and the importance of affected systems. The organization then needs to be constantly adjusting the baseline to new vulnerabilities and threats that crop up. The trick is to pick the tool that most easily allows the organization to automatically enforce that baseline policy once it has been set.

Lumension Security's Approach to Proactive Endpoint Security

Lumension Security offers enterprises a full spate of vulnerability management solutions that address both patch and configuration management. Its technologies provide a proactive way for enterprises to discover IT assets, assess risks through agent- and agentless scanning, remediate vulnerabilities, validate and report. Lumension Security provides a seamless process that evaluates an environment against vulnerability definitions from all of the major standardized databases. It provides automated remediation and the means to enforce a security baseline set by each individual enterprise.