

## **Five Mistakes of Vulnerability Management**

Anton Chuvakin, Ph.D., GCIA, GCIH, GCFA

Vulnerability management is viewed by some as an esoteric security management activity. Others see it as a simple process that needs to be done in conjunction with Microsoft Corp.'s monthly patch update. " Yet another group considers it a marketing buzzword made up by the vendors.

This article will look at common mistakes that organizations make on the path to achieving vulnerability management perfection, both in process and technology areas.

### **No. 1 Scanning but failing to act on results**

The first mistake is scanning for vulnerabilities, but then *not acting* on the results. Vulnerability scanners have become a staple at many organizations. Scanning technology has matured in recent years and the tools' accuracy, speed and safety have improved dramatically. For example, these tools can detect new vulnerabilities from the network side with reasonable accuracy, as well as from the host side with even better accuracy.

However, modern commercial and open-source scanners still suffer from the same disease that troubles early intrusion detection systems (IDS): They are too noisy, since they produce way too many alerts, often false alerts (such as the infamous "false positives"), for various reasons. In addition, they don't tell you what you should do about those vulnerability notices, just as most intrusion detection systems don't tell you whether you should care about a particular alert.

Thus, vulnerability management is not scanning; it includes it, but what happens after the scan is even more important. This includes asset inventory, prioritizing and researching the remediation activities as well as the actual act of patching, hardening or reconfiguration. A detailed explanation of all the important activities goes beyond the scope of this article.

### **No. 2. Thinking that patching is the same as vulnerability management**

It's true that patching is the way to repair many widespread vulnerabilities. Even some industry experts proclaim that vulnerability management is simple: Just patch all those pesky problems and you're done.

However, many vulnerabilities cannot be fixed by simply updating to the latest product version. They require tweaking and reconfiguring various system parameters. Indeed, vulnerability management was born out of a need to intelligently prioritize and fix discovered vulnerabilities, whether by patching or other means.

So if you are busy every second Tuesday but not doing anything to eliminate a broad range of enterprise vulnerabilities during the other 29 days in a month, you are not managing your vulnerabilities.

### **No. 3. Believing that vulnerability management is only a technical problem**

If you think that vulnerability management is only a technical problem, then you're in for a surprise. To be effective, it also involves attention to policy and process improvements. In fact, focusing on process and the "softer" side of the vulnerability conundrum will often bring more benefits than a hi-tech patch management solution.

There are many glaring weaknesses in IT policies and infrastructures. Let's not forget that policy weaknesses are vulnerabilities, too. For example, if you do not enforce a policy for a minimum password length, you have a clear policy weakness, which scanners are not likely to discover and that patching will not resolve.

Thus, weak passwords, lack of data confidentiality awareness and lack of a standard hardened workstation configuration can do more to ruin your security posture and increase your risk than any single hole in a piece of software.

According to Gartner analysts, "the vulnerability management process includes policy definition, environment baselining, prioritization, shielding, mitigation as well as maintenance and monitoring.

Indeed, the vulnerability management process starts from a policy definition document that covers an organization's assets (such as systems and applications) and their users. Such a document and the accompanying security procedures should define the scope of the vulnerability management effort as well as postulate a "known good" state of those IT resources.

### **No. 4. Assessing a vulnerability without looking at the whole picture**

**The fourth mistake** is committed by those who try to follow a proper vulnerability management process, but when they get to the critical challenge of prioritizing the vulnerabilities, they ignore the threat angle of the prioritization. Namely, they try to assess the importance of the vulnerabilities (and, thus, the urgency of their response) based only on the vulnerability itself without looking at the threat profiles and business roles of the affected systems.

For example, a Web server with an unpatched vulnerability deployed in the DMZ where it is subject to constant probing and attacks needs to be patched much sooner than a test system deep in the bowels of the enterprise. At the same time, a critical finance system that is not attacked frequently, but contains data critical to the company's viability (something like the infamous "Coca Cola formula") also needs to be in the first round of patching.

One way to avoid this mistake is to use the risk formula:

risk = threat x vulnerability x value, (what does value mean in this context?) and use the results of such a formula to decide what to patch first. Using a Security Information

Management (SIM) product that implements such vulnerability scoring will help to automate such a process.

To intelligently prioritize vulnerabilities for remediation, you need to take into account various factors about your own IT environment as well as the outside world. Those include:

- Vulnerability severity for the environment
- Related threat information and threat relevance
- Business value and role information about the target system

Recently, a new standard was proposed to classify vulnerability severity and help organizations prioritize their remediation efforts. The <http://www.first.org/cvss/> Common Vulnerability Scoring System (CVSS) takes into account various vulnerability properties (such as priority, exploitability and impact). The CVSS plan promises to provide a uniform way of scoring vulnerabilities, as soon as it is adopted by more vulnerability information providers. However, CVSS data still needs to be enhanced with business value and threat data.

Business information is vital for vulnerability prioritization, since it ties the technical threat and vulnerability data into to the business function. Every organization is different and thus has different critical assets and applications. Attacks against some of them might cripple the business; others will only cause a brief interruption in non-critical operations. In reality, however, life is not that simple, and a vulnerability in a less critical system could be used as a “stepping stone” to later compromise a more critical one.

### **No. 5: Zero days**

**The fifth mistake, zero days**, gives shivers to many knowledgeable security managers. While I’ve noticed a lot of confusion about what constitutes a “zero-day exploit,” the main idea is that it is an exploit that uses a previously undisclosed vulnerability.

So, even if you patch all the known software vulnerabilities you can still be attacked and compromised by intruders who exploit undisclosed flaws.

What can one do? Apart from a sensible vulnerability management program, which includes a hefty amount of hardening – that *might* protect against “zero day exploits” – and careful network and host security monitoring – that *might* make you aware that you’ve been hit – one need to make sure that the incident response plans are in order. Such cases need to be addressed by using the principle of “defense in depth” during the security infrastructure design. Get your incident management program organized and primed for a response to such attack.

Dr Anton Chuvakin, GCIA, GCIH, GCFA ([www.chuvakin.org](http://www.chuvakin.org)) is a recognized security expert and book author. In his current role as a Security Strategist with netForensics, a security information management company, he is involved with defining future features and conducting security research. A frequent conference speaker, he also represents the company at various security meetings and standard organizations. He is an author of a

book "Security Warrior" and a contributor to "Know Your Enemy II", "Information Security Management Handbook" and the upcoming "Hacker's Challenge 3". Anton also published numerous papers on a broad range of security subjects. In his spare time he maintains his security portal at [info-secure.org](http://info-secure.org) and two blogs.