Assessing Risk and Prioritizing Vulnerability Remediation

Vulnerability remediation is a never-ending process, but, even so, security pros can’t plug every hole in every asset and application. The key is to determine which vulnerabilities are most likely to be exploited and the effects such exploits would have on the business. To do this, security pros must know the business and its technology usage and needs intimately, a process that must involve stakeholders across the organization. In this report we recommend the steps that should be taken to determine the risk of vulnerabilities and the lengths to which remediation can and should go.

By Brian Prince
Brian Prince, has spent the last several years covering IT security from a variety of angles. He spent five years covering the topic for eWEEK, and now develops security-focused analysis for a number of publications.
There are a number of products and processes that security pros can make use of to manage vulnerability remediation. The tricky part is figuring out which holes to plug first—a task made more difficult as the sophistication, reach and number of people looking to exploit those vulnerabilities grows. Organizations need to know what they are dealing with in their environment. They need to establish criteria so they can rank assets and applications according to criticality, with the goal of establishing a vulnerability risk score.

This process must bring together the business and IT sides of the house. It also requires a solid understanding of the nature of vulnerability itself. The more devastating an exploit would be to your organization, the higher the vulnerability should be on your patch priority list. Factors to consider include the complexity of the exploit and the ubiquity of the application that needs to be fixed. Something like Java, for example, should weigh differently than an application present on fewer systems. One of the most important considerations when developing any vulnerability risk assessment is whether a vulnerability is being actively exploited in the wild. For this information, organizations can turn to third-party services and security mailing lists.

In this report we provide context around today’s vulnerability landscape and the ways in which security professionals need to marshal organizationwide resources to assess risk and prioritize vulnerability remediation.
Assessing Risk and Prioritizing Vulnerability Remediation

A man is aboard a raft with five holes. Some of the holes are bigger than others, with the biggest of the bunch sending water spouting upward. But even the smallest of holes can sink the raft if left unattended for too long. So how does the man prioritize which of the holes to leave open while he tends to the other four?

The central question in this story is not unlike the challenge IT administrators face when they deal with the problem of remediating vulnerable applications. Making the wrong decision when it comes to remediation management can sink even the tightest-run ship in the IT world, and the problem isn’t going away. On the contrary: A thriving market for exploit kits and application vulnerabilities ensures that an endless number of financially motivated cyber criminals, hacktivists and attempts at corporate espionage will continue to keep security teams up at night. It also means that patching security holes and closing exploitable windows will remain a vital part of enterprise security strategies for years to come.

For organizations of all sizes, prioritizing vulnerability remediation can be the difference between a breach and a repelled attack recorded in security logs. The challenge lies in dealing with the volume of fixes that need to be deployed. Deciding what holes to plug and when begins with organizations understanding their environment: What assets are on the network? Which applications and data are critical? And what’s the risk to the business if...

---

The Severity of Security Holes

A breakdown of the CVSS scores of vulnerabilities in the first half of 2012 shows that most were in the “medium” category.

Source: IBM X-Force
vulnerabilities in these assets, applications and data are successfully compromised?

**The Scope of the Problem**

The sheer number of systems and applications that need to be kept up to date in many environments can make vulnerability remediation management a daunting task. But that is not even the whole story. Attackers and vendors are locked in a constant game of one-upmanship, with sophisticated malware and exploits sold openly. This contest is exemplified by "Exploit Wednesday," the nickname given for the day after Microsoft’s Patch Tuesday. The name is meant as a head nod to efforts by attackers to reverse-engineer the vendor’s security updates to find ways to exploit the vulnerabilities being fixed.

There is some good news: The actual number of vulnerabilities may be declining among the major enterprise software vendors. According to the 2012 Mid-Year Trend and Risk Report from IBM's X-Force research team, the top 10 enterprise software vendors have seen their percentage of the overall number of vulnerabilities drop from 30% in 2011 to 22% in the first half of 2012. However, the same report found that the percentage of vulnerabilities without a patch available in the first half of 2012 was 47%--the highest IBM said it has seen since 2008. The X-Force team speculates that the increase is due to a jump in vulnerabilities in small Web apps and software made by smaller companies.

But it is often not the newer vulnerabilities that catch corporations off-guard. According to a recent report from security vendor Solutionary, 58% of the vulnerabilities targeted by the most popular exploit kits in the fourth quarter of 2012 were more than two years old. The top three vulnerabilities found in
exploit kits were CVE-2010-0188 (Adobe Reader and Acrobat), CVE-2011-3544 (Oracle Java) and CVE-2006-0003 (Microsoft Windows). Though this does not necessarily mean that these vulnerabilities were the most successfully exploited, they clearly are still being exploited. It stands to reason that vulnerabilities that are not yielding any positive results for a hacker would be rotated out of an exploit kit and replaced with new ones.

The cost of not patching can be significant if attackers are able to use a vulnerability to sneak their way past other defenses. A case in point is the well-publicized Operation Aurora attacks from a few years ago, in which hackers used Internet Explorer zero-day exploits to target companies ranging from Google to Juniper Networks to Rackspace.

With the sophistication of attackers and malware showing no signs of decreasing, any drop-off in software vulnerabilities should not be taken as a sign that patching can be taken lightly. On the contrary: The persistence of exploit kits such as Blackhole—which at one point last year was spotted selling for between $1,000 and $4,000 in underground markets—makes it vital that organizations implement an effective patch management strategy.

The Starting Point

Developing a vulnerability remediation management process can be difficult, but, as the old saying goes, the longest journey begins with a single step. That first step should be the identification of critical applications and assets.

"The motto for risk prioritization should be ‘know thyself,’” said Andrew Storms, director of security operations at nCircle. "In order to prioritize any kind of patching you need to identify your critical systems and understand exactly where your business-critical information is. This isn’t always as easy as it sounds—it requires an in-depth understanding of how users interact with critical business information and intellectual property."

Ideally, this is something organizations should already have documented. But, even if they do, it’s good practice to verify this information to make sure that it is up to date. To begin this process, organizations need to identify and group anything with an IP address according to how it functions and what it provides to the business, said Paul Zimski, VP of solution marketing for Lumension.

It should be noted that while understanding the IT environment is a vital part of securing it, the process of mapping the organization in a detailed way can be difficult and fraught with error, said Wolfgang Kandek, CTO at Qualys. "It makes sense to address the obvious mission-critical environments first, but it might then be easier to just secure the general computing infrastructure in an encompassing way, rather than drilling down and deciding on an environment-by-environment basis whether security is required," he said. "Excluding environments from security backfires when security boundaries change or if they were simply mapped incorrectly in the first place."

Closely linked to this should be an understanding of the data in the enterprise—
specifically, where it is and whether it is mission-critical. This information can be used to determine the actual threat of a compromise in terms of its impact on the business. This part of the prioritization process requires input from various parts of the organization, with the conversation centering on a number of issues, including:

>>> How sensitive is the data that could be exposed if the vulnerability is exploited? If there is a SQL injection vulnerability in a Web application, for example, that vulnerability could expose a back-end database. If that database holds sensitive personal or proprietary information, the amount of damage a successful hack could cause is significantly greater than if that database was used to store less-critical data.

>>> Is the vulnerable application business-critical? A customer-facing application may be more important than an application only used internally by employees.

>>> Are there compliance concerns to consider? Compliance regulations like the Payment Card Industry Data Security Standard (PCI-DSS) can ratchet up the danger if an application is compromised. If there is a breach, an investigation may turn up violations that could cost additional money. A recent example of this can be seen in the fine levied against Sony by the Information Commissioner’s Office in the United States in connection with a hack against the PlayStation network in 2011.

In other words, separate the technical risk of
exploitation—which would include considerations such as complexity of the attack vector—from the business risk of a bug—such as the risk it poses to business operations and any financial fallout if a hack were to occur.

This requires involving people in the conversation beyond the IT staff.

"It's important to note that this isn't an exercise that should happen in isolation within the IT department, but rather include both business and technical owners," said Lumension's Zimski. "Without this foundational framework, organizations will be prioritizing based only on what something is technically and not by its impact to business operations and risk."

It is especially important to have executive buy-in. Whether organizations should have a dedicated team in charge of patch management—as opposed to having it handled by a more general desktop support team—will depend on the size of the organization and its staffing levels.

Once an inventory is complete, organizations can begin to assess the places in which security holes exist. Conducting a penetration test and vulnerability scan will give an enterprise a baseline to work from during this process by enabling the security team to understand the current patch levels of the environment. Once that baseline is established, organizations will have a working knowledge of their security and can begin to prioritize what needs to be done.

Now the process of developing a list of security vulnerabilities can truly begin. To do this, organizations should start by bringing together all of the information they have gathered about the company's assets and their criticality. While it may seem smart to begin with the systems and applications that are easiest to attack, a more prudent approach is to start with the elements of the environment that are home to mission-critical data before closing holes elsewhere.

**Determining Risk**

When determining risk, a good place to begin is with the Common Vulnerability Scoring System (CVSS), from the NIST National Vulnerability Database. CVSS scores are computed using three categories of metrics: base metrics, which include factors such as attack vectors and whether an attacker would need to authenticate to exploit the vulnerability; temporal metrics, such as whether a patch is available; and environmental metrics, such as the potential for physical damage or loss of life.

"IT administrators can use the highest CVSS base score of the vulnerabilities addressed in the patch, and then modify it according to availability of exploits and the prior history of the application plus the age of the vulnerability," said Qualys' Kandek.

Some vendors, including Microsoft and Adobe Systems, have their own severity scores that they release with their advisories. For example, in addition to ranking each of its Patch Tuesday security bulletins "critical," "important," "moderate" or "low," Microsoft scores them according to what it calls the Exploitability Index. The index, which Microsoft released in 2008, ranks vulnerabilities...
a 1, 2 or 3. The index is meant to gauge the likelihood that functioning attack code will be developed.

Such scores, however, are not the be-all and end-all of patch prioritization. Rather, they are just one part of the equation that organizations should consider.

Any score or other metric must be considered within the context of the criticality of the application or system in terms of its business value. For example, researchers at BitDefender recently disclosed that attackers were exploiting a previously patched Word-Press vulnerability (CVE-2012-3414) left unfixed in the Yahoo Developer’s Blog as part of an attack that stole session cookies from Yahoo Mail users. The end result of that attack was that hackers were able to get their hands on user contact lists and spam an ever-growing set of targets. When determining priority, the impact of the attack—in this case, spam and hijacked accounts—had to be considered and weighed alongside other factors such as the difficulty of exploiting the issue.

“High-severity vulnerabilities that give the attacker remote code execution capabilities are more likely to be attacked than vulnerabilities that allow only local privilege elevation or leak information,” said Kandek. “If an exploit is available, either underground or publicly, the urgency of applying the patch increases dramatically, requiring IT and end users to apply the patch immediately.”

Determining whether exploits for a particular vulnerability are circulating in the wild is not always easy. After all, zero-day vulnerabilities are not exactly unheard of, and could theoretically be exploited for months or even years before they are uncovered.

This is where security vendors and watchdogs come in. Security teams should monitor security mailing lists such as Full Disclosure to keep abreast of vulnerability research and the release of any exploits or proof-of-concept code that could be utilized by attackers. Security professionals should also consider becoming part of industry cooperatives such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). This combination of raw data and industry and peer context will help your organization put vulnerabilities in perspective.

Indeed, knowledge is power, and the more you can learn about how attacks are developed and what’s trending among hackers, the better prepared you will be to determine a vulnerability’s real risk to the organization. What is being weaponized and what trends attacks seem to be following should carry weight in an organization’s decision about how quickly to patch and remediate a particular issue, said Scott Lambert and Brian Gorenc of Hewlett-Packard’s DVLabs.

“If an adversary has to jump through certain hoops, obviously that affects the kind of risk score that you end up with,” said Gorenc, DVLabs’ manager of vulnerability research.

As mentioned earlier, exploit kit makers have some favorite targets. Typically, these involve the most ubiquitous pieces of
software on the market, such as Java, Internet Explorer and Adobe Reader. These applications are targeted most for a simple reason—their wide use means there are more targets in the line of fire. With that in mind, bugs in these and other commonly targeted products should receive more attention than bugs in applications that are less popular.

"The reverse engineering of security patches requires a close study of the application to understand its inputs and its coding conventions, including the creation and adaptation of internal tools such as fuzzers, etc.," said Kandek. "This is a large investment, and attackers will take it into consideration when choosing what application to attack next. Applications that attackers are familiar with are more likely to be targeted by them again."

Practical Concerns

A number of other practical issues also should be considered. How many vulnerable assets can be fixed with a single patch? Does applying the patch require a system to be rebooted? What effect will that have on the speed of deployment? What needs to be done so that the patch can be tested? What impact will that testing have on the business?

The same priority rankings used to determine the order in which vulnerabilities should be remediated can also be used to determine the priority for testing patches before they are deployed—a must to avoid the pitfalls of a patch disrupting the production environment.

"It’s best to first roll out patches to a small group of production machines that are representative of the overall environment and determine whether or not there are conflicts," said Lumension’s Zimski. "Once those successfully patch machines have successfully been updated without any deleterious effects, then rolling out to the rest of organization can begin. Back-end systems that have rigorous change-control policies in place will need to be put through formal test procedures before deploying any changes."

In the end, the vulnerabilities that rank highest will vary from organization to organization. But what will always be ranked critical is the need to apply patches for serious vulnerabilities in a timely manner.

"Patching is an endless treadmill," said nCircle’s Storms. "Every major enterprise application is always somewhere in the never-ending patch cycle. The key to finding the sweet spot for patching—the patch that will deliver the greatest risk reduction with the least effort—is a comprehensive understanding of where your critical business information is stored. This is where critical patches should be applied first, and the answer to this question differs for each business."
Want More Like This?

*InformationWeek* creates more than 150 reports like this each year, and they’re all free to registered users. We’ll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you’ll find:

**A Guide to Network Vulnerability:** Building a more robust network vulnerability management program can help you identify security holes before an attacker does, as well as develop more secure systems and applications in the future. In this Dark Reading report, we examine the products and practices that will get you there.

**Choosing the Right Vulnerability Scanner for Your Organization:** Blurb about this story goes here fill this space please Blurb about this story goes here fill this spVulnerability scanners can be used to help detect and fix systemic problems in an organization’s security program and monitor the effectiveness of security controls. However, a vulnerability scanner can improve the organization’s security posture only when it is used as part of a vulnerability management program, in which products, processes and people are working together to find, identify, prioritize, and mitigate threats. Here are some tips on choosing and implementing vulnerability scanners in your enterprise.

**Using Google to Find Vulnerabilities In Your IT Environment:** Attackers are increasingly using a simple method for finding flaws in websites and applications: They Google them. Using Google code search, hackers can identify crucial vulnerabilities in application code strings, providing the entry point they need to break through application security. Sound scary? It is, but there is good news: You can use these same methods to find flaws before the bad guys do. In this special report, we outline methods for using search engines such as Google and Bing to identify vulnerabilities in your applications, systems and services—and to fix them before they can be exploited.

**PLUS:** Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek 500* and the annual State of Security report; full issues; and much more.