



Integrating Vulnerability Assessment & Remediation: Guidelines to Maximize Performance and Benefits

In this article, Matt Mosher, Senior Vice President of Americas at PatchLink Corporation will outline the process for successfully integrating vulnerability scanning and remediation capabilities to ensure organizations maintain a secure environment while complying with internal and external security policies.

Over the last several years the explosion of vulnerabilities across all platforms and the shrinking exploit window has left traditional IT security and IT operations teams in a bit of a quandary.

Historically the two teams have been separated by a line akin to the one between church and state. The IT security team is tasked with ferreting out an increasing number of vulnerabilities that could potentially leave the infrastructure exposed. Once they've come up with their laundry list of problems they lob them over the fence to IT operations on the other side. IT operations is then asked to address these issues in between all of the other day-to-day activities involved in keeping the infrastructure running. That may have worked in the past, but today's problem is that security's laundry list continues to lengthen. Over the last three years Windows vulnerabilities have increased by 75 percent and Macintosh holes have skyrocketed by 228 percent, according to research done by McAfee. Meanwhile, the countdown to fix these flaws has been shaved to nearly nil.

"In 2006 we've seen a significant rise in attacks that take advantage of zero-day vulnerabilities, leaving a user or system unable to defend against the attack since no patch is available," noted Marcus Sachs in the end-of-year SANS Top 20 Report for 2006. So not only must IT operations staff fix more problems, but they also need to mend them in a shorter timeframe—all while still maintaining the same level of system availability and reliability as before.

Obviously, something's got to give, and it shouldn't be the security of the systems. Many experts believe that the only way to adapt to the new threat landscape is to develop a proactive set of methodologies that better integrates the two sides of the fence, eliminating the "us and them" mentality that is so pervasive in IT security and operations relationships at this time.

"IT organizations need to become more effective at running cooperative processes across IT security and operations," wrote Mark Nicolett and John Girard in a Gartner report. "The elimination of desktop, server and network vulnerabilities requires a coordinated effort between the IT security and operations groups."

No More Scan-and-Patch

The first step to establishing a more cooperative relationship between IT security and operations is to change the organizational mentality about vulnerability scanning and remediation. Part of the reason why the old model isn't working anymore is because it was never an efficient way to run vulnerability management program in the first place, says Paul Zimski senior director of market and product strategy for PatchLink.

"What you ended up getting into is this constant scan and patch syndrome, where you have one team scanning, another team patching, the other team scanning. It is sort of the rinse-wash-repeat cycle," he says "You're constantly

playing catch-up, you're constantly chasing your own tails, finding new and resurrected old problems and hoping they get resolved."

It is imperative that organizations move away from the scan-and-patch mindset. Not only is it a reactive method of security, but also not every problem can be fixed with a patch. Some may be fixed through a patch, but others problems might best be solved through a configuration change or a policy change. Because of this, administrators need to develop the approach to these risks into a process.

Instead of chasing down each individual vulnerability one-by-one, this process-oriented approach should focus on enforcing policies that mitigate risks to the organization's assets, prioritized by system criticality and the importance of associated business needs. Organizations need to ask themselves what desired state of security they wish to enforce. By focusing and calibrating resources on this single issue, they can achieve a higher level of efficiency with fewer resources because they don't have two different teams finding and enforcing different problems without any common ground.

This increased level of efficiency should help organizations reap the reward of an overall infrastructure that is more hardened against attacks. In fact, a recent Gartner report noted that implementing an integrated vulnerability management program can help to reduce successful external attacks by up to 60 percent.

A vulnerability management program will vary from business to business, but there are a few traits common to the best. First, the organization must involve the right stakeholders throughout the entire process. Second, it must set a mandatory security baseline and policies to enforce them. And third, it must utilize tools and methods that will enable all IT groups to work cohesively in maintaining the baseline.

All three of these developmental elements can go a long way toward achieving the ultimate goal of bringing risks down to a level that the organization can live with. In the end an organization needs to come to terms with an acceptable level of risk, one that balances the health of the network with the health of the business.

Stakeholder Involvement

In order to do it right, whoever is setting mandatory baselines and policies must not only understand the business, but also how IT infrastructure enables the business. Because no single person should be expected to have that level of understanding all on their own, it is best to organize a committee with a diverse membership to drive the vulnerability management program's development. Non-technical representatives from various business units can provide insight into the most strategic divisions and business processes. Members from IT operations can shed light on which systems directly enable those key processes. And IT security members can inform the committee on how to balance the availability and effectiveness of those systems against the threats from the outside.

All of these insights together should help the committee to develop a minimum level of security that the organization is comfortable with and to begin defining IT policies to ensure this baseline is maintained.

