



Remediating IT vulnerabilities: Quick hits for risk prioritization

<http://searchsecurity.techtarget.com/tip/Remediating-IT-vulnerabilities-Quick-hits-for-risk-prioritization>

September 2011

By Diana Kelley

Vulnerabilities are a fact of life, and having to patch or remediate them is an ongoing process at most IT organizations.

But, an organization can't always patch or remediate all IT vulnerabilities as soon as they're discovered. Reasons for this vary: There may not be enough administrative resources; compliance may mandate no changes or patches to the system; or the impacted system cannot be out of service during remediation. And all of that is if a patch is available, which often isn't the case.

How can organizations identify and prioritize exposures and vulnerabilities to isolate those that will have the greatest impact, and deploy their limited resources in the most effective manner possible?

Know your environment

Knowing what services, systems and applications are in the environment is the first and most important step to prioritizing vulnerabilities effectively. A highly critical exploit isn't a concern if it affects applications or systems that aren't in use. Knowing your environment also means knowing the IT architecture and controls that are in place. For example, a database vulnerability may not be a top concern if there are firewalls, database access monitoring and intrusion prevention systems protecting that database from attack. Similarly, if there is a firewall protecting a Web application from a specific exploit, patching that application may be less critical than patching an application for exploits that can't be stopped with other mechanisms.

Finally, consider the criticality of the data and services on the system and the business impact that would result from loss of data or disruption to those services. Fixing a vulnerability on a server that stores publicly available information might be lower priority than fixing one that stores highly sensitive customer data. However, if a disruption to a server with publicly available information prevents customers from doing business with you, it's critical, even though the data might not be.

As Seth Shestack, associate director of information security for Temple University told me, the most important thing is to “Know your environment; what the press says is highest priority may not be what’s highest priority for your own environment.”

Use multiple information sources

To stay on top of vulnerabilities as they are discovered, use information from multiple sources rather than relying on just one. Most software vendors keep a list of known exploits on their sites and communicate this data to licensed users. Vulnerability scanning vendors update their databases with new exploits and provide this information in scan reports, along with severity ratings for exploits that many vendors allow to be customized or tuned to the user’s environment. As J. Wolfgang Goerlich, network operations and security manager for a mid-sized money management firm told me, he looks for reports that provide “solid information regarding what the threats are and at what frequency they’re occurring.”

Public vulnerability repositories, such as the National Vulnerability Database, a “U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP)” and the Common Vulnerability Scoring System (CVSS) calculator can help organizations determine the severity scores associated with a specific vulnerability.

And don’t forget compliance mandates that can affect severity and raise the priority of a particular fix. For example, a vulnerability on a system within a cardholder data environment may be higher priority due to PCI DSS.

Create a remediation plan

Use the environment and metric information to create a normalized remediation plan. At the Visiting Nurse Service of New York (VNSNY), CISO Larry Whiteside and his team stay on a patch-and-fix schedule by placing a metric around new vulnerabilities that takes into account the unique VNSNY environment and other inputs, like the CVSS score. “If it fits in a certain range,” Whiteside told me, “it is critical and will be patched or remediated in 30 days. Less critical scores will be addressed in 60 days – and so on up to six months for very low-priority fixes.”

The time allotted to fix IT vulnerabilities may vary from organization to organization: Some entities require fast cycles of seven days or fewer for highest priority vulnerabilities, while others need longer cycles to accommodate patch and change freezes during audit periods. The key lesson here is to match a priority metric to a specific time-to-fix to provide a documented, repeatable process.

After implementing a fix, use re-scans and tests to validate that the vulnerabilities have been remediated, while also checking for new vulnerabilities in the environment. As the program matures, revisit and revise as needed. Changes in business impact analysis and risk will occur over time: For example, changes to the topology of the environment, new regulations put into effect, and shifting data classification standards. Revisit the risk

assessment and risk prioritization frameworks when these changes occur. Although the basic framework and time-to-fix cycles may not change, new information may place systems in a higher or lower priority ranking.

To keep the fix process focused and effective, know your environment and business impact, create meaningful metrics that take into account public and private ratings, and stay on plan with preset time-to-fix periods.

Diana Kelley is a partner with Amherst, N.H.-based consulting firm SecurityCurve. She formerly served as vice president and service director with research firm Burton Group. She has extensive experience creating secure network architectures and business solutions for large corporations and delivering strategic, competitive knowledge to security software vendors.