IDC ANALYST CONNECTION

Charles Kolodgy

Research Vice President, Security Products

Using Virtual Patching to Optimize Security Management and Reduce Costs

June 2012

Patching is critical to an organization's security posture because it protects against security vulnerabilities. Without software patches, attackers continue to exploit these vulnerabilities. However, the standard patch management process is daunting because of its cost and complexity. Software patching has a significant impact on business operations, including the direct cost of patch management software as well as the indirect costs associated with taking IT staff away from other tasks and downtime. Other business impacts relate to security. There is often a significant delay between when a patch is released and when it can be deployed across pertinent systems. But no matter how quickly the patching process is done, there will always be a window of vulnerability. Many of these concerns can be addressed by virtual patching, which can offer immediate vulnerability protection for any system or application within an enterprise. Virtual patching can be a cost-effective complement to traditional patching processes by reducing disruptions caused by emergency patches, providing protection to unpatchable components, and greatly reducing threat levels.

The following questions were posed by Trend Micro to Charles Kolodgy, research vice president of IDC's Security Products practice, on behalf of Trend Micro's customers.

Q. It is well understood that patch management is an important component of IT security. However, in addition to its benefits, patch management has elements that add to its complexity. What are some of the issues organizations should be aware of?

A. Software must be patched because attackers continue to exploit old vulnerabilities in which patches are available but have not been installed. But the entire patch management process is complex because of the multiple steps it requires. The first level of complexity comes from the size and breadth of an enterprise environment. The more devices and applications an organization has, the more difficult it is to keep track of which patches have been installed, which are being installed, and which still need to be installed. After it is determined that a patch needs to be installed, software must be obtained from the software issuer and then tested to ensure that it doesn't create conflict with other applications. After the patch is tested and validated, it has to be deployed throughout the environment, which often involves scheduling downtime.

Other complexities involve the fact that it is sometimes difficult to get timely patches from vendors after vulnerabilities are discovered. Vendors are focused on developing new products, so patching of existing products isn't always a priority; this situation can be exacerbated when one software vendor acquires another. Another issue is when a critical patch is issued by a vendor outside of its normal patch cycle. Emergency patches must be applied quickly because of the heightened threat.

Q. How does software patching impact business operations?

A. Software patching has a significant impact on business operations, including the direct cost of patch management software. There are many other costs, which are mostly indirect and difficult for an organization to quantify. The most significant indirect cost is tied to IT staffing. The patching process is very time consuming, thus taking IT staff away from other tasks. The second greatest indirect cost is downtime. Most patches will require some time to load, especially on servers. Some organizations might have enough servers to stagger the downtime to maintain operations, but many smaller companies don't have that luxury, so product applications must be shut down for a period of time.

Other business impacts relate to security. No matter how quickly the patching process is done, there will always be a "window of vulnerability" of days and in some cases even weeks between the time a patch is released and the time it is installed. Given how quickly exploits can reach the hands of attackers via automated exploit toolkits, organizations need to respond in kind. However, some businesses choose to postpone deploying emergency patches because of the disruptions they can cause. This is a valid business risk determination, but it does extend the window of vulnerability, which leaves organizations open to possible breaches and their accompanying costs.

Today you can't talk about business operations without considering regulatory compliance. Compliance has a huge impact on IT operations, and it has an impact on patch management too. Many security standards and best practices require that patching remain current. The Payment Card Industry Data Security Standard (PCI DSS) requires that patches be installed within one month of release. These time restrictions for patch deployment put additional pressure on the IT staff to maintain compliance.

Q. Are there devices and applications that aren't addressed by a software patch management system?

A. Software patching doesn't make an organization immune from security breaches. It reduces the chance of a breach, but it does not completely eliminate the threat. One reason is you can't patch all software vulnerabilities. Many systems and applications fall outside the standard patch management system, including legacy applications, out-of-support systems and applications, and embedded components. Legacy applications are generally those developed by organizations either internally or under contract and are very difficult to patch. They often include legacy Web applications, which are a popular threat vector and account for many breaches.

Out-of-support systems are those that have been installed and are no longer supported by the software vendor. Many versions of operating system software, for example, are still in use well past their last support cycle. In these cases, patching is done up to the date of final support, but any vulnerabilities discovered after end of life will have to be addressed either through custom support agreements, which are often cost prohibitive, or without support from the software vendor.

Embedded components, such as point-of-sale terminals, kiosks, medical devices, or SCADA systems, can't be patched because in many cases there is no user-software interaction. A vendor might be able to manually patch the system, but such patching wouldn't be considered timely. Sometimes the cost to patch is too high or someone else is managing the embedded system.

Q. What is virtual patching, and how does it work?

A. Virtual patching provides the functionality of a patch through a series of protections that "virtually" remediate a vulnerability to prevent it from being exploited. A virtual vulnerability remediation consists of multiple layers that provide all of the appropriate protection. The first layer is a bidirectional stateful firewall that filters communications over ports and protocols, passing only what is specifically allowed. This reduces the attack surface. The next level of defense is a finely tuned intrusion prevention system that uses rules to prevent known threats along with behavior analysis and self-learning to protect systems from zero-day attacks.

Because Web applications are a huge attack target, protection rules are needed to secure against threats such as SQL injection attacks, cross-site scripting attacks, and other Web application vulnerabilities. In addition, malware is one of the most prominent tools used by attackers, so the virtual patching solution should have an antimalware component that can detect and block malware. The system should also include some method of integrity monitoring that detects malicious and unauthorized changes to directories, files, registry keys, and other items.

Further, the virtual patching solution needs to have strong management capabilities that can apply appropriate rules to protect a system based on the operating system version, service pack, patch level, and installed applications. This management component should also be able to automatically remove rules after patches are deployed in order to minimize resource utilization. To be most effective, a virtual patching system should offer protection to network resources, cloud components, and servers and desktops, both physical and virtual.

Q. How does virtual patching minimize or resolve the business impacts of conventional patch management solutions?

A. Virtual patching is the perfect solution to deal with many of the business problems and costs associated with standard patching. By utilizing virtual patching as a complement to standard patching, organizations can mitigate many of the issues that raise the costs — both direct and indirect — of standard patching. Virtual patching vastly improves the security of the enterprise by providing protection until a patch can be implemented and by permanently shielding the critical systems that fall outside the standard patching system. It is the ideal solution to protect legacy, out-of-support, and embedded systems.

Virtual patching works to shield zero-day vulnerabilities as well as vulnerabilities that are 1,000 days old. This continuity makes it very easy to maintain a consistent patch program that will not have additional costs. It also means that the "window of vulnerability" is very small. As soon as a vulnerability is discovered, the virtual system can be configured to protect the affected systems without the need to wait until a patch is issued, tested, and deployed.

In summary, virtual patching systems can offer immediate vulnerability exploit protection for any system or application within an enterprise. Virtual patching cost-effectively complements traditional patching processes by reducing disruptions caused by emergency patches, providing protection to unpatchable components, and greatly reducing the "window of vulnerability." Virtual patching provides protection for loss of revenue, brand reputation, customer trust, and regulatory fines that could result in a data breach made possible by an unpatched system. When used in conjunction with traditional patch management systems, virtual patching allows IT greater control over the appropriate scheduling of patches and protects unpatchable systems, optimizing security management and reducing costs.

ABOUT THIS ANALYST

Charles Kolodgy is a research vice president for IDC's Security Products service. In this role, he executes primary research projects and analyzes markets for both vendors and user customers. Mr. Kolodgy's responsibilities within the Security Products service include both hardware and software security products. Product areas of concentration include endpoint security, vulnerability assessment and management, and encryption. Research areas that cut across product markets include product certification, Web site security, threats, and security policy.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

For more information on IDC, visit www.idc.com. For more information on IDC GMS, visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com