From: www.cio.com

How Microsoft's Patch Tuesday Affects Business Processes and Security

– Karen D. Schwartz, CIO

July 09, 2008

Time: The second Tuesday of every month, 10:00 a.m. PST. Like clockwork, Microsoft releases a group of security patches. And like clockwork, that release sets in motion a flurry of events from businesses, security vendors, the media and even hackers.

MORE ON CIO.com
Microsoft Reissues Patch, Encourages XP SP2, SP3 Re-Installs
Microsoft's Critical Bluetooth Patch Didn't Work on XP
Microsoft Releases Massive Set of Security Updates

Microsoft Patch Tuesday, as it is widely known, started in October of 2003 at the request of Microsoft's customers, who preferred to receive patches in an organized way, at a specified time, explains Christopher Budd, Microsoft's security response communications lead. The change was made to make testing and deploying updates easier and more predictable.

In formalizing the process, Microsoft gave customers what they wanted, but in doing so, they also fostered a bustling industry around those monthly patches.

It's a pattern that repeats every month: On the Thursday before Patch Tuesday, the Microsoft Security Response Center (MSRC) issues an advanced notification about what will be included. On Patch Tuesday, customers that have signed up for the Security Notification Service receive a notice alerting them of the newly available security updates. Users can then download the security update using a variety of Microsoft or third-party tools—ones that have sprung up specifically to deal with the complexity of what and how to install Microsoft security patches.

Because of these complexities, an entire industry has grown up around Patch Tuesday. Businesses race to quickly determine which are the most critical for their users and which might inadvertently cause more problems than they solve. Security firms rapidly implement fixes to their own systems and push them out to users. The press floods the public with descriptions and warnings, and hackers work to reverse-engineer the patches to discover and use the vulnerabilities to their own advantage.

"Every Patch Tuesday sets off a race where companies try to get their computers patched before they accidentally hit a website with hacker code," says Brian Livingston, editor of *Windows Secrets* newsletter.

A Necessary Evil

With all of this activity going on, it's no wonder that many companies don't relish the process of

determining which patches are most important to push out to all PCs on the network and which can wait until later. In addition, some patches can cause more problems than they solve, due to incompatibility and instability issues.

"Companies need to learn as much about these patches as they can to know which ones are essential, which can be delayed and which shouldn't be installed under any circumstances," Livingston says.

While very small companies can handle the task themselves, even midsized companies find themselves with a very big problem—one that is often too difficult and time consuming to handle internally. That problem has created a small industry of patch-management consultants and services. These companies, like BigFix and Lumension Security (formerly PatchLink and SecureWave)—as well as Microsoft itself, with Windows Server Update Services—provide software that assess systems' vulnerabilities and allow corporations to properly categorize and prioritize patch installation.

But given the complexity of deciding which patches to install and in what order, sometimes automated solutions don't do the trick. To address this problem, yet another small industry of security experts has sprung up—experts who can do the analysis and testing necessary to quickly give businesses the answers they need.

At the same time that companies are beginning to grapple with the released patches, security vendors like Symantec and McAfee are rushing to document the vulnerabilities. At Symantec, for example, Patch Tuesday sets a flurry of activities in motion; one group documents the vulnerabilities, a second writes signatures that prevent exploitation attempts, and a third team works on file-based detection of any client-side vulnerabilities that may have been patched.

The teams work as quickly as possible to send content to customers as soon as possible—sometimes, within minutes, says Ben Greenbaum, a senior research manager at Symantec of Cupertino, Calif.

But as quickly as businesses and vendors get to work on interpreting and installing the patches, hackers intent on exploiting the vulnerabilities are hard at work trying to reverse-engineer the patches, which help them create new attacks. Some people derisively call this "Exploit Wednesday".

Microsoft's attempts to keep security patches as narrow as possible and to change as little of the binary code as possible to avoid creating compatibility and stability problems, actually helps hackers, says Ryan Russell, a professional hacker who helps decode the world of hackers and is director of information security for BigFix, a security management software company in Emeryville, Calif.

"A typical Microsoft patch updates only a couple of DLL files, which is helpful to the bad guys because they can compare the two binary files and find the one difference between the two, which is the vulnerability," he explains.

What's more, the face of the hacker is changing, compounding the problem. While the previous breed of hacker was looking to disrupt things, get famous or just have fun finding loopholes, the new threat is how companies, organizations or even countries are looking for vulnerabilities to profit more from corporate assets like servers than personal devices like desktops and laptops. That makes the problem even more insidious, says Don Retallack, a lead analyst at Kirkland, Wash.-based Directions on Microsoft, a research firm focused on Microsoft.

All in all, however, many believe that Microsoft's handling of security patches, especially releasing them on a specific schedule, is beneficial to those organizations whose systems are affected. Everybody knows the patches are coming, and companies and vendors are as prepared as they can be.

Still, Livingston says Microsoft receives a failing grade for releasing systems that need patching as often as they do.

"Microsoft needs a much stronger emphasis on security before programs are written instead of adding security to a program after it's done. This step really needs to be taken before the program is released," he says. "The next version of Windows and Office really needs bullet-proof security. There are operating systems like FreeBSD that haven't had remote exploits for years, so it's not impossible to create an operating system that's resistant to attacks from the Internet."