Patchwork Pretty:

Your checklist for a best-practices approach to patch management

InfoWorld Custom Solutions Group

SPONSORED BY: Symantec

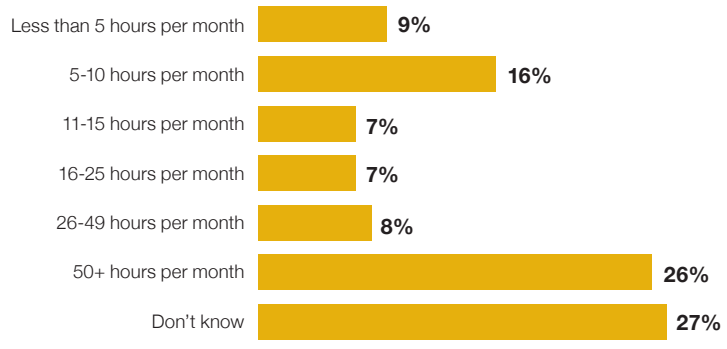
Some aspects of patch management have become almost routine for IT departments managing software, largely due to Microsoft's monthly "Patch Tuesday." Yet in many cases, companies pay little or no attention to some commonly used browsers and applications, perhaps because IT has been overwhelmed by the volume of software requiring regular manual patches.

The importance of updates and patches can't be overrated, however. According to SANS Institute, "Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain."

Vulnerable Outlook

CSO Magazine's annual "Cyber Security Watch Survey" tracks the rate of security attacks and the organizational impact. In 2012, the study found that two-thirds of respondents were more concerned about security threats than in the previous year, and that the average monetary loss due to cyber attacks in the previous 12 months was $324,000, up from $123,000 in the preceding year.

On average, organizations dedicate 27 man-hours to patching third-party applications every month.



SOURCE: IDG Research Services,April 2013

According to Symantec's annual "Internet Security Threat Report," there were 5,291 vulnerabilities reported in 2012, compared with 4,989 in 2011 (a 6 percent increase). Those threats stem, in part, from the fact that many companies and consumers fail to apply published updates in a timely way. All the while, toolkits that zero-in on well-known vulnerabilities make it easy for criminals to target millions of PCs and find the ones that remain open to infection. In fact, the vulnerabilities that are exploited the most often are not the newest.

Attacks aimed at Microsoft products are well documented and numerous due to the overwhelming number of computers using those products. Yet, the list of the most vulnerable software includes popular browsers such as Apple Safari, Mozilla Firefox, and Google Chrome, along with common Web-enabled applications such as Adobe Flash Player and iTunes.

Slippery Slopes

A recent poll of the Infoworld audience, conducted by IDG Research Services on behalf of Symantec, finds that most respondents are patching Microsoft Windows monthly or more frequently. Only about half report patching Adobe products and Java regularly, and the rate for other third-party applications, such as browsers and plug-ins, falls off quickly.

"Most enterprises are starting to get a good handle on patching Microsoft software, but the fact is that most vulnerabilities do not lie with Microsoft today," says Damon Covey, director of regional product management with Symantec. "There is a proliferation of third-party software in the enterprise, and if IT has to manually stage and test and deploy patches for everything, it is a very task-intensive operation."

Barriers to Overcome

In many cases, IT organizations simply don't have an efficient way to analyze what patches need to be rolled out. The IDG poll finds that almost 60%

Between one-quarter and two-fifths of organizations report they are extremely effective at each patch management

	Extremely effective	Somewhat effective	Not very effective	Not at all effective
Analysis (determining which updates will be rolled out to which devices)	39%	46%	14%	1%
Assessment (identification of relevant vulnerabilitites and updates)	36%	46%	15%	3%
Application (timely deployment of updates with minimum business disruptions)	32%	50%	16%	1%
Assurance (compliance reporting)	26%	46%	23%	5%

SOURCE: IDG Research Services,April 2013

of organizations are not fully effective in identifying what vulnerabilities need updates. Indeed, less than one-third of respondents rate themselves extremely effective in the timely deployment of updates to third-party software.

Manual patch management processes can be inefficient and error-prone, and poor application management can result in unacceptable downtime. In the end, IT constantly responds to incidents rather than proactively managing day-to-day procedures.

Taking Control

How do you know when patch management is out of your control? According to Symantec's Covey, the most obvious tip-off is when IT either is uncertain or doesn't know what is running on user devices. Given the ease of obtaining and using "free" applications, IT may not be aware of what resources workers are taking advantage of. For example, 50% of respondents in the IDG survey indicate that in their organization patching doesn't apply to any Google software.

With more and more workers operating remotely, IT may not have the tools to keep tabs on the inventory of software installed on devices being used. "Most tools require some type of VPN or secure connection to maintain an inventory of what is on user devices, but many workers now use the Internet without a secure connection to a remote management server," says Covey.

Another tip-off may be that IT is spending more time on patching, but achieving reduced results or at best treading water. The organizations polled by IDG dedicate on average 27 man-hours to patching third-party applications every month, and less than 10% indicate they've been able to reduce the amount of time on this task from the previous year.

Patch Management Checklist

Symantec recommends a best-practices model that streamlines the process, saves time, improves coordination between the security and operations teams, and enhances the protection of an enterprise's systems:

- **Assessment:** The security team reviews the latest security advisories and identifies the latest updates and patches to create a risk assessment that prioritizes the various updates applicable to their environment.
- **Analysis:** Using the risk assessment, the staff responsible for change management determine the full scope of the rollout and develop a remediation strategy.
- **Application:** Based on the remediation strategy, the operations team rolls out the actual updates and patches.
- **Assurance:** All active participants involved in the first three phases work together toward continuous improvement of the overall patch management process.

Conclusion

With the continuing proliferation of software and devices in the modern enterprise, manual patch management simply can't keep up. Managing Microsoft's monthly Patch Tuesday updates represents just the tip of the iceberg.

Today, effective patch management requires a combination of automation and adherence to a best-practices approach that encompasses all the third-party updates and patches relevant to your organization and can address the needs of both IT security and IT operations. For more information, visit http://www.symantec.com/patch-management-solution. ■