5 BIGGEST MISTAKES IN PATCH MANAGEMENT

1

PUTTING OFF PATCHING

There is no question: you need to patch. Every software product has bugs and many have security vulnerabilities. Unfortunately, people around the world, including security services are trying to find and exploit these holes.

The vast majority of security events are attack vulnerabilities that have already been addressed. In the case of WannaCry, Microsoft had released an update that addressed the vulnerability two months prior to the worldwide attack. By putting off patching, you leave your environment completely vulnerable to exploits and ransomware.

There is no excuse for not having a strong patch management strategy. This doesn't mean worrying about it for a week every time something like WannaCry hits the press. When the next doomsday strikes, you should be completely bulletproof.

2

GIVING ADMIN RIGHTS TO EVERYONE

One approach for patching is giving all users local administrator rights to let them take care of patching. What are the issues with this approach? Will all users install those patches?

We've seen Windows Update reporting 100+ patches waiting to be installed. By giving users administrator rights, you are creating a huge future attack surface. Typically end users are not as vigilant about clicking to links in emails and opening attachments that might now infect their PC utilizing their administrator rights.

Once infected, the local network can be leveraged to distribute the infection. Even in locked down environments, if an application is often having trouble running, granting administrator rights will solve the problem, but create a new huge hole in your security.

It is worth the time to work out the specific permissions needed by an application rather than granting blanket administrator rights. There are far too many risks involved and it is not an ideal strategy for your IT environment.

3

LETTING VENDORS AUTO-UPDATE

Many operating systems and some third-party applications have self-updating technology. This might seem to be a great solution, however if devices are correctly locked down the user may not have permissions to install the updates.

By allowing the vendor to push out updates, there is a chance you will end-up breaking critical business applications. One of the best examples of this is Java updates.

Unfortunately, patches don't go through the same level of software testing that a full software release typically might. This means patches can often have their own significant bugs.

We have seen many examples of companies like Microsoft recalling patches because of major issues. Last month it was reported that a vendor's auto-update system was leveraged to distribute the malicious NotPetya attack.

4

RELYING ON WSUS

Microsoft provides enterprises a great tool to manage software updates: Windows Server Updates Services (WSUS). However, many organizations make the mistake of thinking they are protected because they use this program.

WSUS does not provide sufficient reporting, so as an administrator there is no way to know if you are completely protected. Questions you should be asking:

Has a patch been deployed successfully?

How can I find out my patch compliance level?

Is there any way to show this to management?

WSUS also focuses on distributing Microsoft's own patches, but what about third-party software applications or non-Microsoft operating systems? It's important to always reevaluate your approach.

5

NOT THINKING BIGGER

Even with a locked down security environment or running WSUS, you could still be at risk. What about your Linux and Mac devices? What about social engineering attacks that cause users to give up usernames and passwords? What about third-party applications, such as Adobe Flash and Java?

Often working in IT, you are not even aware a vendor has released a critical patch. Patching is not something you should be worrying about after a major attack like WannaCry. Instead patching should be a standard IT business process to ensure your organization is always protected.

Patch management best practices are crucial. It's important to select a solution that overcomes the key challenges in developing a patch management process.

A VIABLE PATCH MANAGEMENT SOLUTION SHOULD HELP:

- Identify all devices that can access your network
- Determine existing patch levels
- Identify and prioritize new patches
- Reduce IT staff time spent on patching
- Manage your environment, including third-party patches

CLOUD
MANAGEMENT SUITE

- Predictive Patch Management
- Software Distribution
- Remote Control
- Discovery & Inventory
- Inventory History
- Two-Factor Authentication

SO EASY.

IT systems management from the cloud that finds vulnerabilities before you do, and fixes them.

Start a free trial →

ABOUT US

Cloud Management Suite allows you to get the complete picture of your entire IT environment from the cloud. Automatically discover network devices, remotely deploy software applications and automate patch management. A single web-based console allows access to any device from anywhere.

Headquartered in Aliso Viejo, California, Cloud Management Suite is a growing and dynamic organization with offices in four countries and 12 partners in nine countries. For more information about Cloud Management Suite and how we've revolutionized IT systems management, visit **www.cloudmanagementsuite.com**.

CALL
US: +1 (949) 270-1903
UK: +44 (0) 1256-806567

CONNECT
www.cloudmanagementsuite.com
info@cloudmanagementsuite.com