Patch Management

BEST PRACTICES

LabTech®

Why Does Patching Matter?

Simply put, patching is important because of IT governance. As a corporate IT department, you're held responsible when viruses affect users or applications stop working. It becomes your problem to solve.

Securing your organization's end points against intrusion is your first line of defense. With an increasing number of users working while mobile, simply securing your network through firewalls doesn't account for company data that's been taken outside your network perimeter. Proper patching is the best start to securing those devices.

Most IT professionals pay attention to security and patching their users' systems, but how many have a well-honed patch management policy? Patch management is often seen as a trivial task by end users—simply click 'update'. For administrators, there's a lot more to it, and a proper policy is certainly not overkill. But what should a patch management policy include apart from deploying patches?

Read on to learn how to implement patch management policies, processes and persistence. Plus, gain valuable patching resources and tools.

1 Policy

The first step in developing a patch management strategy is to develop a policy that outlines the who, what, how and when of patching your systems. This up-front planning enables you to be proactive instead of reactive.

Proactive management anticipates problems in advance and develops policies to deal with them; reactive management adds layer upon layer of hastily thought-up solutions that get cobbled together using bits of string and glue.

It's easy to see which approach will unravel in the event of a crisis.

The goal of patch management policy is to effectively identify and fix vulnerabilities. Once you're notified of a critical weakness, you should immediately know who will deal with it, how it will deployed and how quickly it will be fixed.

For example, a simple element of a patch management policy might be that critical or important patches should be applied first.

2 Discovery

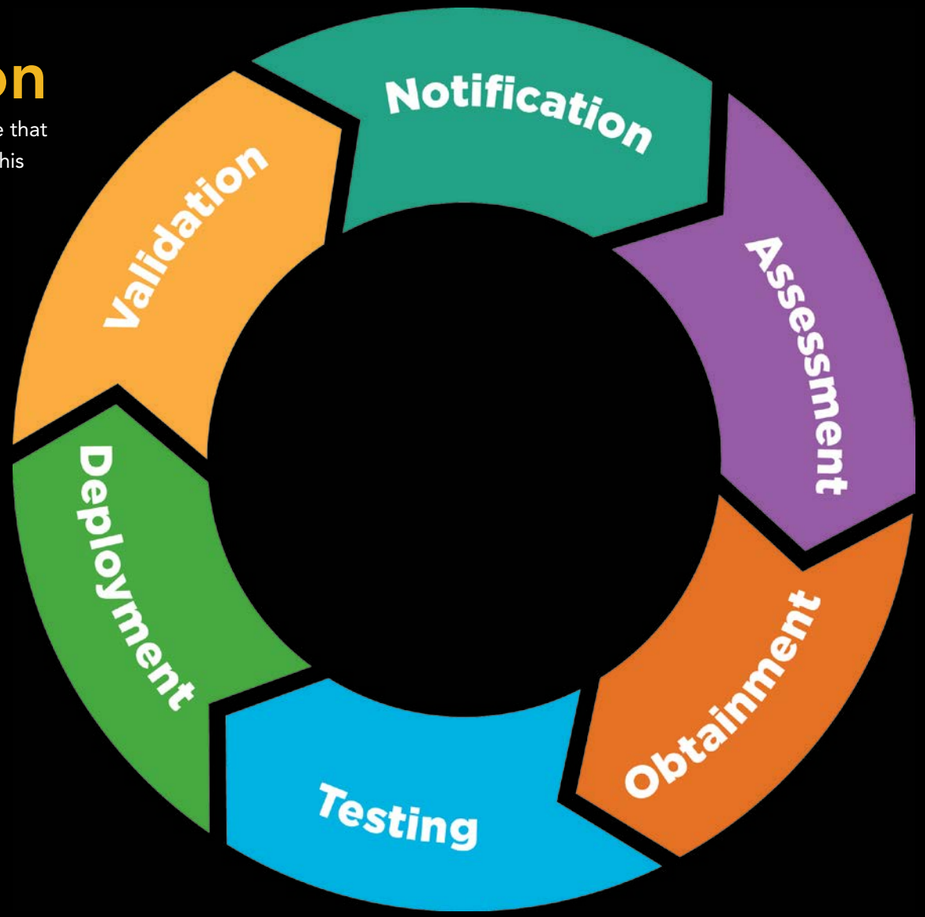
Information comes to you about a newly released patch meant to address a product defect or vulnerability. These notifications can originate from a number of places—LabTech, Automatic Updates, Microsoft's Security Notification Service. It all depends on which tools you use to monitor and keep your systems up-to-date. In this chapter, we'll talk about a number of proven tools you can use to manage patching notifications.

Notification

Notifications might be sent via email from the Microsoft Security Notification Service, a pop-up balloon when you're using Automatic Updates, a message displayed in the Software Update Services (SUS) web console, or some other method. It all depends on which tools you use to keep your systems patched and up to date.

Validation

The final step in the process is often forgotten—making sure that the patch has actually been installed on the targeted systems. This reporting and validation process takes some time, but it is a necessary procedure to ensure that service levels are met.



Assessment

Based on the patch type, rating and a list of potentially impacted systems, you need to decide which systems need the patch, if any, and how quickly they need to be patched to prevent an exploit.

TIP: Having an accurate inventory of systems and applications running on your networks is essential if you want to keep the network secure against intrusion.

Deployment

Avoid applying a patch to all your systems at once, just in case your testing process missed something. A good approach is to apply patches one department or location at a time, testing your production servers after each patch is applied to make sure users and their applications still function properly.

Obtainment

How you get the patch you need depends on which patch management tools you use. In general, tools range from completely manual (e.g. visiting the Windows Update website) to almost entirely automatic (e.g. via client management software).

Testing

In a perfect world, testing should always take place before you apply patches to production systems, especially if you have custom code or line of business applications running on your machines.

TIP: If you need a way to justify the cost of purchasing duplicate equipment for a testing environment, tell the boss it's like insurance. Workstation testing may be a long shot, but how much is at risk if a mission-critical system like active directory stops working?

3 Persistence

Policies are useless and processes are futile unless you persist in applying them consistently. Network security requires constant vigilance, not only because new vulnerabilities and patches appear almost daily, but because new processes and tools are constantly being developed to handle the growing problem of keeping systems patched.

Effective patch management has become a necessity in today's information technology environments. Reasons for this necessity are:

- The ongoing discovery of vulnerabilities in existing operating systems and applications
- The continuing threat of hackers developing applications that exploit those vulnerabilities
- Vendor requirements to patch vulnerabilities via the release of patches

These points illustrate the need to constantly apply patches to your IT environments. Such a large task is best accomplished following a series of repeatable, automated best practices. Therefore, it's important to look at patch management as a closed-loop process. It is a series of best practices that have to be repeated regularly on your networks to ensure protection from exposed vulnerabilities.

Patch Management requires:

1. Regular rediscovery of systems that may potentially be affected
2. Scanning those systems for vulnerabilities
3. Downloading patches and patch definition databases
4. Deploying patches to systems that need them

LabTech Software

4 Patching Resources

Microsoft updates arrive predictably on Patch Tuesday (the second Tuesday of every month), which means you can plan ahead for testing and deployment. You can get advance notice by subscribing to the security bulletin, which comes out three business days before the release and includes details of the updates.

The following is a list of currently available resources you can use when augmenting your patch process, as well as some that can keep you informed of patch-related updates that fall outside the scope of Microsoft updates.

Microsoft Security TechCenter
http://technet.microsoft.com/en-us/security/bb291012.aspx

SearchSecurity Patch News
http://searchsecurity.techtarget.com/resources/Security-Patch-Management

Oracle Critical Patch Updates and Security Alerts
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

PatchManagement.org (Patch Mailing List)
http://www.patchmanagement.org/

Patch My PC (third-party, free patching)
http://www.patchmypc.net/

5 Patching Tools

Client Management Platform

Approving and deploying patches on individual machines is simply not scalable. As your organization grows, it is important to utilize a tool that can automate your patch management process, so your technicians aren't bogged down with the mundane task of individually patching each machine.

A client management platform with built-in patch management capabilities can help.

When searching for the right tool, remember to look for one that enables you to:

Identify, approve, update or ignore patches and hotfixes for one or multiple devices at a group level

Define patch install windows for an individual device or a group of devices

Schedule patch installation times and patch reboot times

Create tickets for all successful patch install jobs

Provide detailed reports of patch install jobs to your management team

Third-Party Patching Tools

It is important to ensure timely installation of patches, so security holes remain closed not only in the Windows operating system, but also in software products that are used on desktops and servers. A third-party patching tool such as App-Care or Ninite can be used for obtaining, testing and deploying updates to third-party applications. Be sure to look for a third-party patching tool that integrates seamlessly with your client management platform for increased automation and efficiency.

Summary

Patch management is a critical process in protecting your systems from known vulnerabilities and exploits that could result in your organization's systems being compromised. Viruses and malware are just two examples of aggressors that take advantage of these weaknesses and can be especially destructive and difficult to correct.

Patches correct bugs, flaws and provide enhancements, which can prevent potential user impact, improve user experience and save your technicians time researching and repairing issues that could have already been resolved or prevented with an existing update. Users generally understand that their systems need to be patched, but they often do not have the expertise to comfortably approve and install patches without help. Developing best practices to manage the risks associated with the approval and deployment of patches is critical to your IT department's service offering.

About LabTech Software

LabTech Software is the brainchild of an IT professional who struggled with the usual challenges and inefficiencies of a reactive IT maintenance and support model. LabTech—its flagship solution—was born out of the urgent need to eliminate technician inefficiencies and the desire to provide preventive and proactive service for an organization. Developed with cutting-edge, agent technology, LabTech is the only global client management platform created by system administrators for system administrators to automate your IT services and eliminate inefficiencies. For more information, please visit labtechsoftware.com or call 877.522.8323.

4110 George Road, Suite 200 | Tampa, Florida 33634 | 877.522.8323 | labtechsoftware.com

LabTech®