

Taking the Pain Out of Patching

Is security patching giving your IT team a headache? Here's a patching panacea from David Beesley, director of consultancy Network Defence

Just like taking regular exercise and flossing teeth, security and vulnerability patching is something that IT managers know that they need to do – but many don't get around to doing as often as they should.

A recent survey of 200 senior managers at companies with under 300 staff by UK analyst firm Quocirca found that less than 30% use any kind of automated process for patch management – the reason usually being lack of resources, perhaps coupled with lower understanding of the importance of patching.

The problem is that patch management is a resource-hungry task which has to compete with day-to-day system maintenance and security tasks. And even though IT staff acknowledge the importance of patching, the issue of finding the time and resources to do it remains.

Just researching the 4,000+ vulnerabilities published by security monitoring body CERT in the last year would demand hundreds of man-hours – and that's before work even starts on applying those patches. And although a member of IT staff may be online regularly to see what patches are released, they cannot be 100% certain that all systems are properly patched.

Time is tight

In IT, time really is money. Recent research from analysts at The Yankee Group put a figure on the time involved in patching – an estimated \$1 million to manually deploy a single security patch in a 1,000-node network environment. The costs include the manual labour involved in fixing problems and downtime while patches are applied.

But as the interval between a vulnerability being discovered and exploited shortens, patching is now a necessity. The 2004 Blaster worm was released just 18 days after

the vulnerability it exploited was discovered, and the pace is stepping up. Later in 2004, the Bofra worm was developed within a week of Microsoft discovering a vulnerability that let malware propagate via online banner ads

So if businesses have to take the patching pill, how do they make it easier to swallow? What strategies can they use to respond effectively to the patching challenge, without consuming too many resources?

Patching panaceas

The first step in approaching patching is to risk-assess the business. The IT team should have the latest snapshot of all of its IT assets, and any vulnerability which apply to each component. This overview can then be broken down into which systems are critical, which should be patched first and which need constant patch maintenance. Tools such as Microsoft Security Baseline Analyser can be used to test if relevant patches have been installed on the network. As an example, a supermarket group may not want to apply non-critical patches in November and December because these are the busiest times of the year, and the risk of downtime caused by new software is unacceptable.

The key point here is to prioritise. For most companies, even those with security patch management solutions in place, patching everything straight away is not an option. The IT team has to be able to cope with the work in progress, and to have the capacity to address any issues which arise during the patching process. In each case, it's worth establishing how big the hole is to be patched. How severe is the risk to systems? Does the patch require other system upgrades first? Try and make the task as bite-size as possible, so you can easily back-track.

So deal first with the systems that are most prone to attack or hacking – such as ecommerce systems, mail systems and critical business applications. Then move down the chain to non-critical systems. It's important to factor in timing of maintenance too – for example, those systems used by office staff should ideally be patched out-of-hours.

Test drive

It may seem a belt and braces measure, but you shouldn't assume a patch will work automatically. Even patches from the most reputable vendors have not been tested in every possible environment. For business-critical environments, these patches

should be tested in a non-production lab. Alternatively, tools such as VMware are valuable, enabling patches on business-critical systems or components to be tested in virtual environments first. Following a successful test, do a trial roll-out of the patch first if possible, to ring-fence any risk from the new patch.

When it comes to rolling out the patches, MS Server Update Services (SUS) can help in deployment. SUS is a free download that automates hotfixes and security patch rollouts. In effect, it's a server that contacts Microsoft and automatically downloads the latest patches, which IT staff check through, approve for use on the network and push out to clients machines.

Insurance policy

Once the initial audit and priorities have been taken care of, the IT manager or CSO should develop a patching policy based on the work done – specifying what patches should be applied, to which systems, and in which order.

The policy should have two elements – one dealing with routine, non-critical patching issues in a routine maintenance cycle, and a second 'emergency' plan for non-routine, critical patches that have to be installed quickly. This gives a script for staff to follow, making it easier for them to integrate patching into the overall IT workflow. Use of an event management application like Microsoft's OM 2005 can help with manageability of networks, giving event management, monitoring and reporting.

In conclusion

Patching is, of course, only one element of an overall security strategy. However, it also makes pivotal contributions to reducing a myriad of vulnerabilities resulting from hacking to helping resolve issues arising from spyware and malware. By following these pointers, companies can ensure they are less likely to fall victim to attacks of any kind. Now that's a sweeter pill to swallow.