

Business Plus Article Jan 2004 Patchwork curtains: The Art of Windows Patch Management

Patches - Helpful things. They help smokers quit smoking, they give teachers jackets distinctive leather elbows, and they prevent hackers from doing untold damage to your IT systems and wrecking your business.

Unless you are struggling with a 90 a day habit, the last one is probably the most critical.

But what is a patch, in the wacky world of computers? Basically, a patch is a modification to the original software to fix a problem. Kind of like touching up a paint job. Most software packages have bugs in them of some form. Some of these are a mere irritation, but sometimes they can create huge problems that wreak havoc on a global scale.

Microsoft Windows 2000 has over 30 million lines of program code. XP has even more. Even though Microsoft spent millions of dollars testing it in every conceivable situation, inevitably there will be mistakes in there somewhere. Given how many people use Microsoft Windows, and how many people have it in for Sir Bill, it is also inevitable that sooner or later these bugs will be found and exploited.

In some cases these bugs can be used to crash a system (known as a Denial of Service or DoS attack). In other cases they can allow an attacker to run programs on the affected computer, stealing or damaging data, or even turning it against the world, becoming part of a legion of computers attacking someone else on the Internet. Either way, being exploited is not good.

People used to assume that they would never be targeted, so why worry? Unfortunately these days, exploiting these holes can be automated to the point that computers can just scan the Internet looking for anything they can exploit. Whether they have heard of you or not. More commonly, the exploit is built into a virus or a "worm" such as "Blaster" which sweeps through the Internet like wildfire doing huge damage.

Even if you have good, up-to-date Anti-Virus software running, it may not be able to stop these "worms". Virus scanning software looks at the files you open on the computer. These exploits don't even need a file, they merely instruct your computer to download and execute the attackers program.

So what do you do about it? How do you know when there are patches you need to apply? Well, that depends on what resources you have available. Modern versions of Windows have a tool called "Windows Update" built in, which will check with

Microsoft and tell you which patches you need to download and apply. You can even automate the

process and tell it to just apply them without telling you. Great! you cry. but as always there is a catch.

Patches are produced by a division of Microsoft called QFE (Quick Fix Engineering). Their job is to resolve the problem as fast as possible. The time between a bug being found and a virus being written to exploit it could be very short indeed. Unfortunately, that doesn't leave much time for testing the patch.

While Microsoft have gotten quite good at this, it is not unheard of for them to release a patch which breaks something else.

So ideally, before applying a patch, you would look at what it is there to fix, and decide if it applies to your computer. You might also look for reports on the Internet of other users who have had problems with it. If possible, you should test the patch on a few of your machines to see if it breaks anything. All this weighed up against the ticking timebomb of a hacker or virus damaging your system if you don't apply it and it is relevant.

Fine, but many companies simply do not have the resources to do this. Even if an IT manager does have time to check out a patch, how do they then persuade their users to download and apply the right ones? Fortunately there is a solution. Several companies produce software to allow the IT manager to push approved patches out to all the computers on the network, without having to go round them all. Microsoft produces a product called SUS (Software Update Services) which does just that and is free to download.

Hoorah! Shout the companies with IT managers. Those without might be less enthused. Fortunately a Bradford based computer company has a solution to this. For a £50 per month subscription, they download and test the patches on a "representative sample" of computers. They scour the Internet for reports of problems, and make a judgement as to whether a patch is safe and relevant to apply. An automated agent running on a subscribers server will then download the approved patches and push them out to every PC on the network.

Hey Presto, hands free patch management for the masses. Currently, this service only covers Microsoft Windows (which is the usual target of these exploits). This will be extended shortly to cover popular packages such as Microsoft Office, Exchange and SQL Server. Please contact the Chamber if you would like further details.

However you do it, your business does need to stay on top of these patches. As anyone who experienced the Blaster or SoBig virus's recently will know, the consequences of not doing could be devastating.