next I.T.

The Importance Of Having A Patch Management Strategy

For Both Microsoft and Third Party Applications

Patching holes in your network is a little like putting a plaster on a cut to make sure it doesn't get bigger!

When it comes to upgrading and patching software and applications, it's fair to say that people get lazy. How many times have you clicked 'later' instead of 'install now?' The problem is that if you fail to patch your Microsoft software and thirty party applications when prompted, you could be putting your business at risk of security breaches.

In order to ensure that your software, applications and overall I.T. infrastructure remains secure, you will need to develop a patch management strategy. Here we explain the importance of having a patch management strategy in place and what it needs to cover.

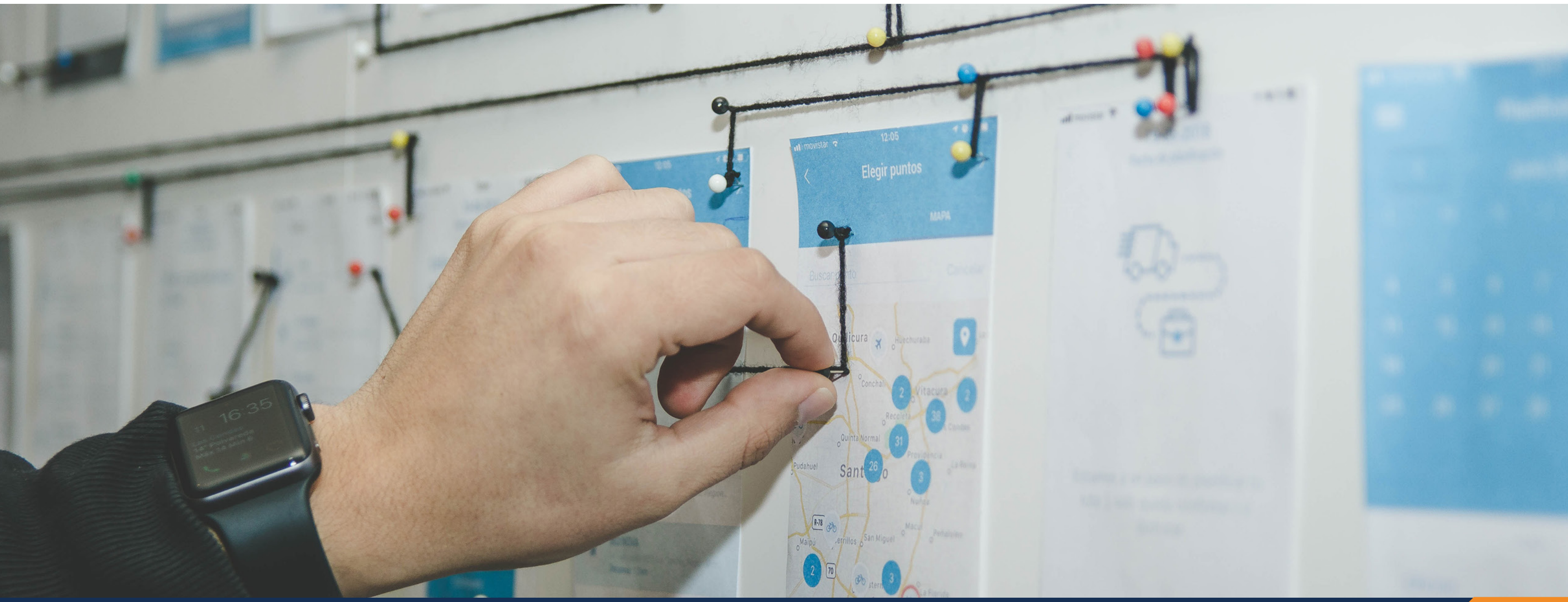
What does patch management involve?

A patch management strategy (or policy) is necessary to the upkeep of your I.T. system's security. It involves testing your Microsoft software and other third party applications to see if there are any flaws that could pose security risks.

If this is the case, you will then have to install relevant patches to the software or applications in order to keep your system safe against malware or other attacks.

Core tasks associated with patch management include:

- Keeping up to date on the availability of new patches (scanning)
- Identifying what patches are right for your Microsoft software and applications
- Installing patches correctly (remediating)
- Testing your system after installation to check for flaws
- Rolling-back to pre-patch settings in the event of an unexpected consequence
- Documenting all related procedures (reporting)



Benefits of a patch management strategy

Businesses will greatly benefit from having a set patch management strategy in place. Next I.T. recommends implementing a set process that your I.T. team must follow when updating and maintaining your system is more likely to result in software and applications being kept up to date and secure. If vulnerabilities are exposed or a problem arises, your I.T. team will know exactly what they need to do in order to rectify it to ensure that your business remains compliant with regulations and standards.

Having a patch management strategy and action process in place is likely to prevent your business from becoming vulnerable to common malware attacks and data hacking. A well planned strategy will not only save your business time and money, but could also save its reputation.

What should your strategy cover?

When creating a patch management strategy for your business, there are various areas that you will need to cover. Below we have provided a brief outline of four of the key aspects you will need to consider.

1. Analyzing applications and identifying patches

The first question your strategy needs to address is which patch releases are relevant to your business applications? In order to do this you will need to analyses or scan your Microsoft software and third party applications. You will then need to identify the security issues and what software updates and patches are available to you to fix these.

2. Communication with software and application vendors

In order to know when an upgrade or patch is being released, you will need to keep in contact with key software and application vendors. It will be the vendors that distribute information about potential security issues and the patches they have created to resolve them. Microsoft issues regular updates via its Download Centre and typically releases major security patches on the second Tuesday of each month, which is unofficially known as 'Patch Tuesday'. Be sure to sign up to vendors' email subscriptions and keep an eye on their websites and blogs.

3. Compliance

Part of your patch management strategy should involve making sure your I.T. systems are compliant with relevant regulations and standards. These include Payment Card Industry (PCI) and Data Security Standard (DSS) Compliance, and HIPAA for healthcare. Remember that regulations and standards are updated over time, so you will need to continuously carry out compliance checks on your software and applications to ensure everything remains in order. If you suffer a data breach and are not compliant, you could be fined or sued

4. Implementation and testing

Your patch management policy should outline the procedures for implementing and testing your Microsoft software and other applications. This will ensure that the installation of patches is carried out successfully and that your I.T. team knows how to test the patches to ensure they are doing their job of keeping your I.T. system secure. Patch management software applications, such as LabTech can help you with some or all aspects of a patch management program.

Outsourcing patch management

It does not matter how big or small your business is, patch management still remains a necessary process:- If however, you do not have the budget or resources to conduct patch management in-house, you could always consider outsourcing it to I.T. expert like Next I.T.

Call or email us at

1 866.388.6398
sales@next-it.net