The Importance of Windows Updates

We have all seen the classic yellow shield and exclamation point (now a notification flag in Windows 7) that indicates there are Windows Updates available for installation, but do you know how these updates actually affect your computer? With Microsoft setting to patch a record 49 vulnerabilities on October 12th of 2016, we believe it is critical to our clients' security that they understand a little about these patches and how you can keep your systems protected. (Don't have time to read? Call us at 618-624-1138 ext. 201 for the solution: Patch Management with Ellegent's SystemPulse Remote Monitoring and Management System)

What are Microsoft Updates?

Microsoft's Update is a service that allows for the periodic patching of system files to address known issues with Microsoft products early every Wednesday morning. Originally called **Windows Update**, it was specifically focused on Operating System patches for Windows. More recently however, it has been expanded to include all Microsoft products and the name has changed to **Microsoft Update**, allowing the automated patching of non-OS software such as Internet Explorer and Microsoft Office.

Microsoft Updates are organized into several categories:

- **Security Updates** - These updates patch security vulnerabilities that could allow a system to become compromised. Security updates are classified as Critical, Important, Moderate, Low, or non-rated. Critical Security Updates are perhaps the most important updates to apply to your system. Ignoring these could leave your computer or server extremely vulnerable to hackers and malicious code.
- **Critical Updates** - Critical Updates fix any major issue that is found in Microsoft products that could cause software errors or unexpected behavior. Together with Security Updates, they form the "High Priority" category of updates from Microsoft and should be set to download and install automatically.
- **Software Updates** - Non-critical issues, such as extended features and minor bugs, are addressed using Software Updates.
- **Service Packs** - Service Packs contain a rollup of all patches to date for a specific piece of software or operating system and usually have additional feature changes. For example, Windows XP Service Pack 3 is the latest service pack for XP and addresses all updates prior to its release as well as a small number of new features.
- Each update has an associated Knowledge-Base (KB) number that gives details on the changes. Security updates will also have a Microsoft Security Bulletin (MS) number associated with them.

Why Should I Update?

Simply put, Microsoft Updates prevent problems. Although there are occasions when updates cause a new issue to appear, generally speaking they "help" more than they "hurt". Not only do Microsoft Updates fix known bugs in software and operating systems, but they plug critical security holes that could drastically affect your security. Microsoft vulnerabilities are actively exploited in countless viruses, which could have been easily prevented by maintaining updates.

How Can I Stay Secure?

There are several methods for maintaining your Microsoft updates, depending on your technical expertise

Use Automatic Updates - All recent Microsoft Operating Systems have an Automatic Update feature built-in that allows you to define a time to

download and install High Priority updates. Although simple to configure there are several drawbacks to using this method:

- All High Priority updates get applied without any intervention. While this may sound like a good idea, updates can often conflict with existing software or may fail and cause other issues.
- Other updates are not applied automatically, such as some software updates and service packs. We have found that it is common to see client computers missing several beneficial updates because no one took the time to install them manually.
- Automatic Updates can be disabled by the end-user, and often are. Without a centralized method for managing updates, they can easily be disabled by an end-user and leave the entire network vulnerable. This is very common and is the cause of many out-of-date machines.
- **Use centralized update software** - Server-based update applications such as Windows Server Update Services (WSUS) can resolve many of the shortfalls that come with having each computer responsible for updating itself. However, there are also some limitations:
- Setup requires a high level of knowledge in order to be successful. From the initial installation to configuring rule sets, approval policies, and memberships, configuring a WSUS server can be very challenging for non-IT personnel. When it is configured, it is often done incorrectly, resulting in clients not receiving some or all patches.
- The local storage requirements on the WSUS server can range from 15GB through to 70GB at present. The processing and storage overheads can easily overwhelm an older server.
- Requires maintenance from experienced IT staff. Whether it is routine reboots on the server itself or checking reports to verify updates are being processed, maintaining a WSUS server can add complexity to your network and an extra workload to your staff.

Use a managed service provider (Preferred) - By far the simplest and most effective way to maintain your updates is to source this cumbersome task out to a managed service provider such as **Ellegent's SystemPulse Patch Management Solution**. Our trained specialists can monitor your patch status remotely, apply needed patches as soon as they are available and tested, safely reboot critical servers within pre-specified maintenance windows, and troubleshoot any update issues that arise. When we test, we use powerful information from our patch database to help determine which patches may cause issues on your systems, if we miss something; we roll back or disable these patches until a new version is released. This takes the process and responsibility of patching completely off the shoulders of your internal employees and places it in the hands of experienced IT professionals.

How Do I Sign up for Patch Management?

Getting your company into a Patch Management program using **SystemPulse** is as simple as a phone call. For a low monthly fee we will deploy our monitoring agent and not only provide you with Patch Management, but you'll enjoy other benefits such as 24/7/365 monitoring for system failures and instant access to our team of professionals for remote support.
Call us today at 618-624-1138, extension 201 for more information.