Tech Solutions INC. Managed Services Computer Consulting Network Administration

TechPoints

November 2014 *IT Tips and TechSolutions News* Vol. 4 No. 11

In This Months TechPoints

Windows Server 2003 Is Now in the Crosshairs

By Dan Ayars, Marketing Coordinator, TechSolutions

Now that Windows XP has been put out to pasture, Microsoft has set its sights on Windows Server 2003 (WS 2003), with the plan to end support for that operating system in 2015. Like they did with Windows XP back in April, Microsoft will stop providing fixes to security vulnerabilities in the software, making it far more susceptible to malicious attacks. The overwhelming industry recommendation is to move away from WS 2003. So for those still using WS 2003, I wanted to take a few minutes to outline what is happening, why you should care and what you should do about it.

What is happening?

On July 14, 2015 Microsoft will cease providing security updates for WS 2003. Conventional support for the product was already halted several years ago with Microsoft only providing security updates since that time. After July 14, 2015 they will no longer provide assisted technical support, software updates and security patches.

Why should you care?

The big thing to be concerned about here is security. All of us here at TechSolutions, are constantly keeping our ears to the ground for changes and developments in the tech world. Regarding the death of WS 2003, the consistent message across the board is to stop using WS 2003 by July 14 or you'll be far more exposed to malicious attacks. Just recently the Computer Emergency Readiness Team for the U.S. Department of Homeland Security issued an alert for WS 2003 that contained this warning, "Using unsupported software may increase the risks of viruses and other security threats. Negative consequences could include loss of confidentiality, integrity and or availability of data, system resources and business assets."

The internet villains of the world, like any criminal, look for weaknesses to exploit. Almost weekly you hear in the news about security compromises where some criminals have figured out a weakness in software and gained access to sensitive data. You don't need an expert to tell you what common sense already does. And common sense, along with the experts, is saying that these crooks are preparing and waiting to attack WS2003 after July 14, 2015. Does that mean the next day all hell will break loose? Not at all, but over time it is expected that attacks on the software will increase and will become more successful because Microsoft is no longer providing the tools for counterattack.

Almost as important, if not more so, is the matter of compliance. I read an article that said after July 14, 2015 WS 2003 will no longer be able to pass a compliance audit. If you have to meet compliance requirements for regulatory organizations or certain clients, then you'll have to outline a game plan to maintain compliance or risk becoming non-compliant.

What should you do?

Don't stick you head in the sand. It's not just us sounding the alert, everyone in the industry is suggesting you upgrade. Achieving a smooth, minimally disruptive migration takes time, planning and coordination. Upgrading a server is different than upgrading a workstation because you are impacting an organization, not just an individual. On the other hand, maybe you'll be one of the few cases where upgrading may not be the best course. Your next step should be to gather the facts from us and other sources, like your software vendors, so you can make a sound decision.

Call or email us to get an idea of the cost and what's involved. Do that sooner rather than later, so if you upgrade there is enough time to get this done right. We will have several clients migrating and will be able to transition any of our clients who choose to do so, however as the deadline nears our schedule will become less flexible. So at a minimum start to determine now what is involved for your specific situation, then you'll have the facts to develop a solid transition plan.

License Audit Emails from Microsoft

One of the biggest IT expenses for many small businesses is software. Some companies require thousands of dollars of software, which can quickly compound when you hire new employees. Businesses who have purchased Microsoft software may soon be receiving a letter from the tech giant asking for a systems audit. Here is a quick overview of this letter and what you should do if you receive one.

The Microsoft Software Asset Management Review

Earlier this year, Microsoft announced that they will be sending out over 30,000 letters to small businesses who have purchased Microsoft software licenses. These letters or emails are focused on checking that you have the right number of licenses for your systems.

This program actually has three audit elements, or emails, that are being sent out to businesses.

1. Internal self-audit email - This is the most common letter businesses have been receiving. It asks them to verify that they are compliant with Microsoft's licenses, which is usually done by sending Microsoft the software keys for each license or product purchased. They then compare this to their records.
2. Software Asset Management (SAM) Engagement - This is a voluntary process where Microsoft sends a Software Asset Management partner to your business to audit your systems and see if you are over or under licensed. For companies who do agree to this, the audit is paid for by Microsoft. The downside is, if you are found to be non-compliant, you will likely face a fairly large bill.
3. Legal Contract Compliance (LCC) audit email - This audit can be enacted by Microsoft if you put off a SAM or self-audit for an extended period of time. Essentially, this is a legal audit that you must comply with. If you are found to be non-compliant under this audit, you could face stiff legal penalties.

What happens if I receive one of these emails?

Should you receive one of these emails you will be asked to carry out the audit by a set date. Most of the emails contain a spreadsheet that you will need to put your license information into. This can take time because you will likely need to physically check every machine using Microsoft software for relevant information. One advantage for our PointCare clients is that we can quickly generate hardware and software inventory reports to assist in this process.

Auditors who come to your business will ask you for network and server access and any other form of information they think they can ask for.

Should you be found to be non-compliant or under-licensed, you will likely then be presented with a bill for the extra licenses. If you happen to be highly under-licensed, this bill could be quite large.

What should I do if I am worried about this audit?

An audit like this could be time consuming, costly, and above all is frustrating for any business owner. What we recommend is working with us. We can help ensure that your business is using appropriate licenses and, should you face a request to do an audit, we can help you through the process.

Published with permission from TechAdvisory.org

Overview of Mobile Payment Systems

Businesses, like restaurants, boutique fashion stores, and even some delivery operations have flocked to mobile payment systems largely because you don't have to invest in expensive Point of Sale equipment and can instead run it all from a device like an iPad. With the recent new mobile payment announcements and continued enhancements, it is highly likely that mobile payment solutions will see explosive growth in businesses the world over.

What exactly is mobile payment?

Most people would define mobile payment as either using your mobile device as a wallet, or using mobile devices to accept payment. Many services allow users to link credit cards to their mobile device and simply scan it over a pay terminal to have their account charged.

Companies on the other hand usually pay a set per-transaction fee in order to use the system; something along the lines of, or slightly cheaper than, most credit or debit-based payment terminals. If you are considering switching over, here is a brief overview of the most common payment solutions.

PayPal

In late September, Internet auction giant eBay announced that they will be spinning off their popular Internet payment system PayPal sometime in 2015. While many users will utilize PayPal to pay online, there is actually a mobile payment solution called PayPal Here, which is expected to grow immensely.

With Here, you get a payment solution app with a card reader that plugs into most smartphones (Android, iPhone, iPad, Android tablets) and allows you to accept multiple types of payment from anywhere you have an Internet connection. You can even track cash payments and record checks.

Vendors can use this app free of charge, however they are charged a 2.7% per swipe fee, based on the amount of the transaction.

Apple Pay

Apple Pay is Apple's recently announced mobile payment system that utilizes NFC (Near Field Communication) on the iPhone 6. Users with an iPhone 6 will be able to link their credit cards to their phone and then will hover their device near a terminal and press their thumb on the device's fingerprint reader to pay.

Your payment information (This is an account number linked to your card. Apple has noted that actual card numbers are not stored.) is stored in the Passbook, and will be accepted at an initial 220,000 stores in the US. There is a good chance that small to medium businesses will be able to integrate this solution into their business in the near future, so it would be a good idea to keep an eye on this.

What is interesting is that many banks have announced that they are considering accepting, or will accept Apple Pay as a method of payment. This means that businesses with an existing NFC payment terminal – which is often provided by a bank – should be able to accept payment (if the bank does of course). Rumors have it that merchants will not be charged a transaction fee to use this service.

Square

Square is arguably the most popular, or at least the most well-known, mobile payment system. With a card reader that is compatible with most popular mobile devices (Android, iPad, iPhone) users can set up a whole Point of Sale system via the Square Stand and accept a wide variety of payments.

To use this solution, you need either the card reader (which is free) or the Square Stand (which costs around $99). For each transaction there is a fee that starts at 2.75% for credit and debit cards.

Amazon's Local Register

Introduced in mid-August, this new card reader is aimed at both PayPal and Square solutions. As with these, there is a card reader that can be plugged into most devices (Android, iPad, iPhone) and an app that goes along with it. Businesses with the reader can then use the device to accept payment.

Where this solution differs is that the reader costs $10 to purchase. That being said, the $10 is refunded towards your first transaction fees upon signing up. The transaction fees are also quite a bit lower with businesses paying a flat rate of 2.5% per transaction (based on the total transaction amount).

Google Wallet

Google Wallet is a hybrid mobile and online payment solution that allows users to add credit cards to their wallet and pay for things either online, or at stores with NFC payment terminals (also called contactless terminals).

While most users who have made a purchase on Google Play, or have used their Google Account to make a payment have used Wallet, this hasn't been the most popular of solutions when it comes to customers using it to pay in-store. The reason for this is because there are only a limited number of devices with the required NFC radio (two to be exact). This system is also currently limited to the US only. Customers around the world can use Google Wallet to pay online however.

There is a good chance that with the recent new announcements and upcoming mobile payment products, Google will be pushing this out to more devices in the near future.

There are other mobile payment system options available, so it is a good idea to contact us before you implement one. We can help you not only find a solution that works for your business, but ensure that it can be integrated into your existing systems.

Published with permission from TechAdvisory.org

Cleaning Computers and Devices

Computers and mobile devices might be high tech but they are still exposed to dust and grime and get dirty after a time. While for many a slightly unclean screen is a minor annoyance, neglecting to clean your devices could result in a decrease in longevity and possibly performance too. Once you commit to regularly cleaning your tech equipment it is important that you know how.

Cleaning desktop monitors

The monitor on your desktop is what many people spend the majority of their days in the office looking at. A clean monitor makes it easier to see your desktop more clearly. The best way to clean your monitor is to turn it off first, then take a microfiber cloth (these can be purchased at many optical stores as well as computer stores) and gently rub in a circular motion.

If there are still spots, then dip the cloth in a tiny bit of water – don't spray the water onto the screen – and try cleaning again. It is important that you don't press hard on the screen, as this could damage your monitor's pixels. Also, it is not a good idea to use paper-based products like paper towel or tissue, as they will not only leave residue, but may actually scratch the monitor slightly.

Cleaning mobile screens

Mobile and other touch screens usually will get your fingerprints all over them, making it harder to see what you are looking at. The best way to clean these screens is with a microfiber cloth. For tougher to remove spots you can dip the cloth into a small amount of water and then gently wipe the screen. Don't splash water onto it before cleaning, as water could get inside the device, which will likely void the warranty while potentially ruin internal components.

Some people suggest rubbing alcohol to remove fingerprints and disinfect the device. While this will be ok for some screens, many manufacturers recommend against it because the alcohol can eat away at the protective film on some devices.

If you notice that there is a lot of dust or gunk on the edges of your screen, or even in cracks, you may need to take the device into a mobile shop for further cleaning. Do not open the device yourself as this could void the warranty.

Cleaning your keyboard

Our fingers are touching keyboards almost all day, and after a while you will notice that your keyboard gets a bit grungy, with debris and dirt even between the keys. Before you do start cleaning, be sure to unplug the keyboard, or turn it off if it is wireless. To clean the upper parts of the keys – where your fingers strike the keys – try dipping cotton swabs into rubbing alcohol and then cleaning the keys with a gentle rub.

To clean between keys you will need compressed air which can be purchased at most office supply and computer stores. Spraying in between keys should be enough to get rid of most of the dust and grit.

Cleaning your mouse

Like the keyboard, the mouse can get quite dirty too, with grime from your fingers and dust in general. The best way to clean a mouse is to first unplug it and then use cotton swabs dipped in rubbing alcohol to

gently clean it. You should not need to open your mouse and most models are designed to not be opened by users.

Cleaning your laptop's body

If your laptop's body is dirty the most effective way to clean it is to turn it off, unplug it, and clean it with cotton swabs dipped in rubbing alcohol. Some online articles recommend using a Mr. Clean Magic Eraser, or similar cleaning tool. While this does work, it acts in the same way as super fine sandpaper, so you have to be careful that you do not end up actually lightly scratching the body.

Cleaning your computer tower

Some people may want to clean their desktop computer's tower. While this is doable by taking a slightly damp microfiber cloth and wiping down the front and side of your tower, we strongly recommend avoiding the back, and certain areas of the front, as there are ports and components that could be easily damaged.

As always, be sure to disconnect the power source and all wires before cleaning, as any water damage could ruin your computer.

Cleaning the inside of your computer

Dust will eventually get into the inside of your computer and could clog up cooling fans, causing them to stop working properly. This can potentially lead to other components overheating. The internal components of your computer are extremely fragile and need to be handled with great care. Do not take the case off of your computer as this usually voids your warranty.

Published with permission from TechAdvisory.org.

TechPoints is a monthly newsletter from TechSolutions, Inc.

Editor: Dan Ayars, Marketing Coordinator, TechSolutions, Inc.

TechSolutions, Inc. ● 5630 Kirkwood Highway, Wilmington, DE 19808 ● www.TechSolutionsInc.com ● (302) 656-8324