October 2014

TechTidbit.com

brought to you by Tech Experts

Are You Ready For Windows Server 2003 End Of Service?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Next July will mark the end of Windows Server 2003 Extended Support. What does that mean for you if you're a current owner of Server 2003?

It means that there will be no more security patches or updates, putting your whole business at risk of new threats or viruses as well as potential performance problems due to incompatibilities with newer software and applications.

The bottom line is that if your business still uses Windows Server 2003 you will need a plan soon. Analysts are estimating that 10 million machines are still running Windows Server 2003 and that they will soon be stranded, especially those serving regulated industries as they will need to maintain the security and confidentiality of these servers.

For these reasons, it is important to look into the needs of your business. Here are a few considerations:

Cost

With the end of service to Windows Server 2003, the cost of required tools to keep your systems online, such as intrusion detection systems, more advanced firewalls, etc. will make buying Windows Server 2012 a cheaper alternative.

Security

The end of service will put your business at risk since there will be no fixes for bugs and viruses or patches for system vulnerabilities.

Compliance

Certain professions require regular audits to be done in order to fulfill regulation requirements.

Mounting compliance expenses as well as the price of audits will make the upgrade to Windows Server 2012 another cheaper alternative.

What are your options?

The only option available right now is to migrate your data from Windows Server 2003 to Windows Server 2012.

The migration must be performed by professionals in order to ensure the safety of your data, especially because this migration will involve a move between 32-bit and 64-bit platforms.

In summary, it is important to look ahead and ensure that you take steps to protect your business way ahead of the July 2015 deadline.

Tips To Protect Your Business PC From Malware

Michael Menor is Vice President of Support Services for Tech Experts.

In today's online world, technology users are essentially in a state of near-constant attack. Almost every day, there's a new data breach in the news involving a well-known company and, quite often, fresh rules for protecting personal information are circulated.

Because of malware in email, phishing messages, and malicious websites with URLs that are one letter different from popular sites, employees need to maintain a high level of awareness and diligence to protect themselves and their organizations.

Phishing activities are especially pervasive, including attempts to steal users' credentials or get them to install malicious software on their system. The astonishing success rate of phishing attacks makes them a favorite.

Why? More than 70% of people will follow the link to a phony website and, of those that followed the link, 30%-50% will routinely give up their usernames and passwords.

Many like to think of the network perimeter with all its firewalls and other fancy technologies as the front line in the cyber war, but the truth is there's a whole other front.

Every single member of a company's staff who uses email or the Internet is also on the front line and these people are generally considered a softer target than hardware or software. It's simple: if the bad guys can get an employee to give up his or her user credentials or download some malware, they can likely waltz right past the technological controls, basically appearing as if they belong there.

When using a computer for personal functions, a user generally has to have the ability to install software and modify the system configurations. Typically, such administrative functions are not available to all users in a corporate environment.

As a result, even if an organization has made an effort to improve a system's security, a user doing work on a personal computer has the ability to disable and circumvent protections and has the privileges to allow for the installation of malware.

As companies migrate toward a world of bring-your-own-device policies, some companies are developing strategies to help address these risks. But, as a rule, using a work computer for personal reasons or doing work on a personal computer (or tablet or smartphone) can significantly increase the threat level that an employer has to protect itself against.

To help their organization protect systems and data, employees need to implement some smart web browsing habits. Smart web browsing means engaging in the following activities:

Beware of downloads

Malware can be hidden, not just in applications or installation programs, but in what appear to be image and video files also. To limit the likelihood of downloading content that contains malware, only download from reputable sites. With sites that are not a household name, take the time to do a little research and see if other people have had issues.

Additionally, be sure that antivirus software is set up to automatically scan downloads. Or scan downloads manually, even when receiving them from name-brand sites, as it is not unheard of for infected files to make their way onto otherwise legitimate web sites.

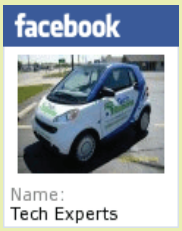
This is especially true for file-sharing sites where the site owner cannot control every piece of content a user may place there.

Be wary of deceitful sites

Those running sites already breaking the law by illegally distributing copyrighted materials -- like pirated music, movies or software -- probably have no qualms about including malicious content in their downloads or stealing information.

Continued on page 4

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

When Nature Strikes – Is Your Ark Ready to Float Your Business to Dry Land?

Scott Blake is a Senior Network Engineer with Tech Experts.

Flooding can strain the resources of even the most well-equipped organizations. Natural disasters give little warning to companies, so *preparing* for the disaster is the only way to reduce the high cost of rebuilding.

Have a plan ready and in place

Disaster recovery plans are now becoming a requirement for many industries. To be prepared, businesses need to locate and define the regulatory requirements of their individual industry. In addition to reducing hardware damage and data loss, this will help avoid fines, penalties or negative press associated with noncompliance.

The health care industry has begun to require that hospitals have a recovery plan in place. The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) sets standards for operating a health care organization and evaluates the industry to ensure that these standards are met. Documented and field-tested recovery plans for theft, vandalism, loss of critical data, provision of emergency power, and file and flood recovery are now required.

Trying to implement or even design a plan while in the middle of a disaster will only lead to a less than successful recovery. Make sure your team is ready for action and everyone knows what to do. It's better to be overprepared than have a plan with holes that will sink your business.

Your data: Make sure you have it

Back up your data regularly. Manage a duplicate copy of all data, programming, and company processes at a different physical location or in the cloud. That way, you can continue working at a secondary location if your system crashes.

One way to do this is to keep copies of all your data, programs, bare metal backups and virtual machines in data centers in other states or in some cases different countries.

Tech Experts offers encrypted, HIPAA-approved, online backup of your files, documents, folders and data bases. If you require bare metal backups or the ability to convert your server into a virtual machine to keep afloat until replacement hardware is in place and running, Tech Experts also offers devices that can fulfill that requirement as well.

Treat your data like your money

Keep it safe and keep a lot of it.

Power: Must have it

An uninterruptable power supply (UPS) and a generator provide consistent backup power for your business if power lines go down. Make sure you routinely test and service them to ensure they're working correctly.

Electrical components, including service panels, meters, switches, and outlets, are easily damaged by flood water. If they are underwater or come in contact with water for even short periods, they will probably have to be replaced. Make sure all of your computer systems -- from servers, workstations, backup devices, and UPS's -- are up off the floor. Servers, backup components and UPS's should be at least four feet off the floor.

Another problem is fires caused by short circuits in flooded areas. Raising electrical system components helps you avoid those problems. Having an undamaged, operating electrical system after a flood will help you clean up, make repairs, and return to your property with fewer delays.

Good relationships with vendors, customers and partners

Create strong relationships with your partners, vendors and customer base. In good times, they will give you access to new ideas, technologies, and business opportunities. During a crisis, they're a security blanket with teams of people who know your business model and have resources to help you rebuild.

Insurance: Business is life

Floods and water damage are expensive. Business insurance is crucial and it's not only for physical property. The right kind of insurance will replace lost income as well. Make sure your business insurance policy is up to date and has the correct coverage to support your business in crisis mode.

If you have questions or you're looking for suggestions on prepping your business for recovery, call Tech Experts at 734-457-5000.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Considerations When Buying A Home Wireless Router

Choosing and buying a router for your wireless internet at home can be a frustrating experience; you want speed, performance and coverage as well as longevity in the life of your upgraded router.

It's not an easy task if you add to it the complexity of all those numbers attached to the router and the knowledge required to install it.

So, here are few considerations that will help you choose your next wireless router:

What's the end goal?

Ask yourself: why am I buying a router? If it's simply to build a wireless network at home and have access to the Internet, you could probably get away with a router at under $200.

However, if you want extra features, such as added security, parental controls, the ability to connect USB printers, and added external storage drives for data sharing, you need to search for a higher end router.

Also, you may not even need to have a wireless router in your house, especially if you use a PC or laptop that is already connected to a cable or DSL modem and there are no other devices that need to be connected wirelessly to the internet.

Should you go for a single or dual band?

Bands are the frequencies in which wireless communications operate. A single-band is geared toward simple wireless networks and a dual-band router operates on both the 2.4 and 5 GHz frequencies.

Although a router that sustains the 5 GHz frequency will work great for gaming and online streaming, it is not as good as the 2.4 when it comes to distance. So, consider the distance you need to cover when choosing the required band.

Further considerations

When buying your next router, remember that soon enough the 6th version of the Internet Protocol (IPv6) will be here, so you will need a router that supports this transition.

Another consideration is extra features that a router may offer, such as SD card slots and USB ports for printers for example.

If you want to future-proof your investment, make sure you get an 802.11 AC router, which is fast becoming the standard in wireless networking.

Finally, even with home networks, the more security, the better!

Tips To Protect Your Business PC From Malware, Continued

Many popular web browsers today have built-in functionality that provides an alert when visiting a website that is known to be dangerous.

And if the browser doesn't give a notice, the antivirus software may provide that function. Heed the alerts!

Employees need to protect their devices from online and in-person threats. Start by keeping the company's system patched. Configure it to automatically apply updates or issue notifications when there are updates and then apply them as soon as possible. This doesn't just apply to the operating system. Keep all installed applications updated; sometimes this takes a little extra work.

Remember, the challenge of security is that the bad guy needs to find only one hole in a security system to get past it, so fix them all. Think of it as putting dead bolts on doors, but leaving the basement window wide open.

To that end, security professionals like to debate the usefulness of today's antivirus software. And it's true that malware continues to become more sophisticated and harder to detect. But it always amazes me how old some of the malware running around is. As a result, use antivirus software and keep it up-to-date.

Also, use a software firewall, either the Windows firewall or one provided in an antivirus package. This is especially true for laptops connected to public wireless access points at hotels or coffee shops, but it also applies to home systems. It just provides that extra layer of defense.

And finally, please, don't ever give passwords to anyone. Be vigilant and question anything new, especially emails and forms in the web browser that request work credentials, no matter how nicely the request is made.