E-NEWS

www.E-Safetech.om | 1-412-944-2402 | © 2018 E-Safe Technologies All rights reserved.

November 2018

In this issue...

When Microsoft stops supporting Windows

Microsoft only supports each version of Window for a certain period and the end of its support for a software product can be a significant challenge for businesses. Currently, Windows 7 is on "extended support" until January 14, 2020. What does it mean when Microsoft terminates support of your Windows version? Let's have a closer look.

No more security updates

End of support for Windows means Microsoft stops issuing security updates for that operating system (OS). For example, Windows Vista and Windows XP can no longer receive security updates despite the substantial security holes found in them.

On January 14, 2020, the same will be true for Windows 7. From there, you'll be on your own. You can still use antivirus tools and other security software for protection, but they won't be enough to defend against bigger threats. Security software will also gradually drop support for older versions of Windows. Large organizations can sign "custom support" contracts to keep getting security updates while they transition to a new OS. But Microsoft will ratchet up the price going forward to encourage those organizations to move to a new version of Windows.

Software companies will halt support too

When Microsoft ends support for an OS, that's also the signal for third-party companies to stop supporting that particular version of Windows with their own software and hardware. This doesn't happen immediately but it does eventually.

For example, Windows XP support ended on April 8, 2014, but Chrome didn't stop supporting Windows XP until April 2016, two years later. Mozilla Firefox stopped supporting Windows XP in June 2018. Steam will officially drop support for Windows XP and Windows Vista on January 1, 2019. On the other hand, software companies dropped support for Windows Vista more quickly, as it was much less popular than Windows XP.

New hardware may not work

New hardware components and peripherals will stop working on your system too. These need hardware drivers, and manufacturers might not create those hardware drivers for your old, out-of-date OS.

Presently, the latest Intel CPU platforms don't even support Windows 7 and 8.1. However, the operating systems are technically still in "extended support." You can keep using your old OS with your current software and hardware, but you have no guarantees of future updates or compatibility.

When will Microsoft end support?

Microsoft has a well-defined support lifecycle for its software products. They come ahead of time so they're never a surprise. The agreement includes the assurance that Microsoft is committed to providing products with improved security. While they may be unable to provide security updates for older products, they do advise customers to install the latest product releases, security updates, as well as service packs to remain as secure as possible.

Upgrading is better than using unsupported Windows

The support lifecycle is rapidly fading away as Microsoft shifts to its Windows as a service and Office 365 subscription models. If you want to prevent security frustrations, it's best to upgrade to a newer version of Windows. Should you need help in upgrading, or have further concerns about your current Windows, give us a call.

How to protect your Office 365 data

Office 365 is a complete cloud solution that allows you to store thousands of files and collaborate on them, too. In addition to its productivity features, the service comes with security and compliance solutions that will help businesses avoid the crushing financial and legal repercussions of data loss. However, even with its comprehensive security tools, the service has some data security risks that need to be addressed. The following tips will keep your business data private and secure.

Take advantage of policy alerts
Establishing policy notifications in Office 365's Compliance Center can help you meet your company's data security obligations. For instance, policy tips can warn employees about sending confidential information anytime they're about to send messages to contacts who aren't listed in the company network. These preemptive warnings can prevent data leaks and also educate users on safer data sharing practices.

Secure mobile devices
Since personal smartphones and tablets are often used to access work email, calendar, contacts, and documents, securing them should be a critical part of protecting your organization's data. Installing mobile device management features for Office 365 enables you to manage security policies and access permissions/restrictions, and remotely wipe sensitive data from mobile devices if they're lost or stolen.

Use multi-factor authentication
Don't rely on a single password to safeguard your Office 365 accounts. To reduce the risk of account hijacking, you must enable multi-factor authentication. This feature makes it difficult for hackers to access your account since they not only have to guess user passwords, but also provide a second authentication factor like a temporary SMS code.

Apply session timeouts

Many employees usually forget to log out of their Office 365 accounts and keep their computers or mobile devices unlocked. This could give unauthorized users unfettered access to company accounts, allowing them to steal sensitive data. By applying session timeouts to Office 365, email accounts, and internal networks, the system will automatically log users out after 10 minutes, preventing hackers from opening company workstations and accessing private information.

Avoid public calendar sharing

Office 365's calendar sharing features allow employees to share and sync their schedules with their colleagues. However, publicly sharing this information is a bad idea because it helps attackers understand how your company works, determine who's away, and identify vulnerable users. For instance, if security administrators are publicly listed as "Away on vacation," an attacker may see this as an opportunity to unleash malware on unattended computers.

Employ role-based access controls

Another Office 365 feature that will limit the flow of sensitive data across your company is access management. This lets you determine which user (or users) have access to specific files in your company. For example, front-of-house staff won't be able to read or edit executive-level documents, minimizing data leaks.

Encrypt emails

Encrypting classified information is your last line of defense to secure your data. If hackers intercept your emails, encryption tools will make files unreadable to unauthorized recipients. This is a must-have for Office 365, where files and emails are shared on a regular basis.

While Office 365 offers users the ability to share data and collaborate, you must be aware of potential data security risks at all times. When you work with us, we will make sure your business keeps up with ever-changing data security and compliance obligations. If you need help securing Office 365, we can assist you, too! Contact us today for details.

The lowdown on cloud security

If you're thinking of transitioning your business to the cloud, consider the security of the platform. While providers would like us to believe that the friendly, fluffy cloud image used to market the service means it is automatically secure, the reality is far different. Just ask one of the nearly seven million Dropbox users who had their accounts hacked. This is not meant to scare you, but to make you aware that cloud security needs to be taken seriously especially if you're a business owner. To help you make a smooth and safe transition, we've put together a list of precautionary measures you can take to ensure cloud security.

Ask your IT provider what cloud security policies they have in place

This is probably the single most important security measure you can take. Find a trusted IT provider and have a candid conversation with them about their cloud security policies.

Ask where the physical cloud servers are located

When you have "the conversation," don't forget to ask about this. Believe it or not, some cloud servers may not even be located in your own country. Wherever they are, it's wise to make sure they're located in a safe data center with proper security afforded to them.

Create unique usernames and passwords

Your login credentials represent one of the cloud's main security vulnerabilities. Think of a better password than "12345" or "football."

Use industry standard encryption and authentication protocols

IPsec (Internet Protocol Security) is a reliable technology choice.

Encrypt data before it's uploaded to the cloud

Encryption is a must, and can be done by you or your cloud service provider. Should hackers manage to access your data, they'll find it useless because they can't make heads or tails of it.

When it comes to trusting the security protocol of a cloud service provider, transparency is key. They should take security seriously, be able to explain their security policies clearly, and be willing to answer any questions. If they can't do one of these, that's a red flag telling you to find another vendor.

Are you ready to talk cloud security and transition your business into the cloud? Call us today. We're happy to answer all your questions.

Outdated firmware: An overlooked threat

If most of your company's computers are obsolete, they double or even triple your chances of experiencing a data breach. This emphasizes how dangerous it is to have outdated applications, operating systems, and even web browsers. Failing to update your firmware could expose your business to major security threats.

What is Firmware?

Firmware is a basic type of software that is embedded into every piece of hardware. It cannot be uninstalled or removed, and is only compatible with the make and model of the hardware it is installed on. Think of it like a translator between your stiff and unchanging hardware and your fluid and evolving software.

For example, Windows can be installed on almost any computer, and it helps users surf the internet and watch YouTube videos. But how does Windows know how to communicate and connect with your hardware router to do all that? Firmware on your router allows you to update and modify settings so other, higher-level pieces of software can interact with it.

Why is Firmware Security Important?

Firmware installed on a router is a great example of why addressing this issue is so critical. When you buy a router and plug it in, it should be able to connect devices to your wireless network with almost zero input from you. However, leaving default settings such as the username and password for web browser access will leave you woefully exposed.

And the username and password example is just one of hundreds. More experienced hackers can exploit holes that even experienced users have no way of fixing. The only way to secure these hardware security gaps is with firmware updates from the device's manufacturer.

How Do I Protect Myself?

Firmware exploits are not rare occurrences. Not too long ago, a cybersecurity professional discovered that sending a 33-character text message to a router generated an SMS response that included the administrator username and password.

Unfortunately, every manufacturer has different procedures for checking and updating firmware. The best place to start is Googling "[manufacturer name] router firmware update." For instance, if you have a DLink of Netgear router, typing "192.168.0.1" into a web browser will allow you to access its firmware and update process, assuming you have the username and password.

Remember that routers are just one example of how firmware affects your cybersecurity posture. Hard drives, motherboards, and even mice and keyboards need to be checked. Routinely checking all your devices for firmware updates should be combined with the same process you use to check for software updates.

It can be a tedious process, and we highly recommend hiring an IT provider to take care of it for you. If you're curious about what else we can do to help, give us a call today!