September 2018

TechTidbit.com

brought to you by Tech Experts

What Can Companies Do To Prevent Privacy Violations?

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

Whether it's physical, virtual, or in the cloud, discovering and blocking sophisticated threats in the network is at the forefront of every company's mind.

However, businesses are finding that more and more data violations are taking place when network security centers on the edge of the network are not giving equal protection to the network itself.

Security at the perimeter of the network has received most of the attention from data protection companies.

What many internet service providers and businesses have neglected is protecting what lies within the network. What can your company do to solidify your network and protect you from hackers on the inside?

5 Ways to Prevent Privacy Violations

Prevent Data Theft with Patches

If a company's IT department is inattentive when it comes to the application of patches, security vulnerabilities and other bugs can easily creep into a network. A patch is simply a set of changes to a computer program and its data that are created to update or fix a liability or get rid of a virus threat.

Rapidly growing networks today are comprised of a wide range of networks, including the IoT and the cloud. Keeping track of the equipment inventory and the maintenance of this vast network can be a daily trial. For a company to protect its technology, applying patches is no longer an option but a necessity.

Protecting a Network with NIDS

With cloud computing as a way of life, cloud computing security is a mandatory requirement. Network-based Intrusion Detection System (NIDS) is one of the solutions for enhancing the security aspect of cloud computing services.

NIDS discovers and monitors attacks within the network. NIDS is a signature-based technique with an identification data packet throughout the network.

Using Behavior-Based Analysis

Zero-day attacks to a network occur within a time frame, known as the vulnerability window. They are vulnerabilities that have not yet patched the software containing the weakness.

Hackers can engineer malware that exploits compromised systems and steals valuable data. New high-level attacks are operating various techniques to evade protective measures and attack the network connections without even being noticed.

Installing Web Application Firewalls

Although many attacks are caused by phishing emails or known, unpatched vulnerabilities, web-based attacks are becoming more the norm. Software that probes and calculates information directly in the data center is commonly targeted.

A web application firewall (WAF) is a filter that is designed to go before you and sift through incoming traffic detecting potential threats and malicious activity. It is one of the most common means of protecting against attacks at the application layer.

Incorporating Network Segmentation

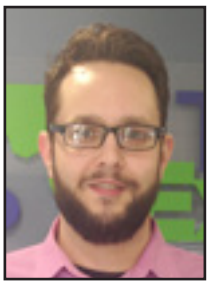
The modern network needs to be able to handle access through varying devices and an assortment of application and data flows. Businesses can markedly improve their network safety by installing Internal Segmentation Firewalls (ISFW).

Network segmentation works by splitting a computer network into subnetworks. If the defense perimeter is breached, an access point penetrated, or if there is an attack from inside the network, ISFW prevents the spread of such threats.

What many internet service providers and businesses have neglected is protecting what lies within the network. What can your company do to solidify your network and protect you from hackers on the inside?

Windows Fall Update 2018: How To Prepare & Avoid Downtime

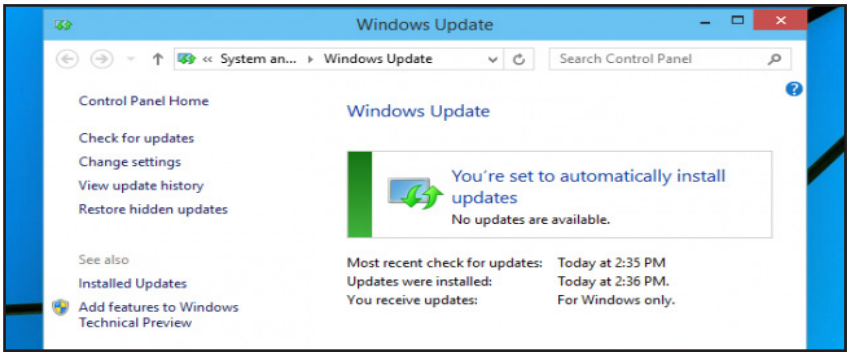
"As with updates in the past, there is a possibility that any of these new system changes will cause issues with different existing applications and processes. 2017's Fall Creator's update was the culprit behind numerous applications failing, even people having to do full system restores for no real reason."



Jason Cooley is Support Services Manager at Tech Experts.

Here it comes again. Windows is coming back with another large feature update for Windows 10, named Redstone 5. As always, Microsoft is attempting to give people more of what they want and better the user experience.

The upgrades and changes slated to hit this fall vary greatly, from a dark theme for File Explorer to the new Windows 10 smartphone integration feature.



While there may be a little something for everyone, what can you expect your experience to be? We can start by examining the numerous changes coming our way this fall.

The first new feature is Clipboard history and sync. By pressing the Windows key and V, you can open up Clipboard history. Allowing all of those copy and pastes you've been doing to be easily recalled. This feature will be great for some users and some will never utilize the functionality.

For an IT professional like myself, I spend a lot of time copying and pasting different things in, not limited to passwords. This brings up many questions, including, "How secure will the sync between devices be?" and "Will any personal information be safe to copy and paste this way, when there is an obvious trail left?" This remains to be seen, but the potential for usefulness, if secure, is exciting.

Another new feature I mentioned earlier is the Dark Theme for File Explorer. This feature allows the color of File Explorer to be changed from white to black. Eyes rejoice! Many people find browsing files and even reading easier to do with a black background and white font. If the brightness is just too much for you to look at day in and day out, then this feature is for you! There is no downside or issue I can see with this feature, as it is purely cosmetic.

Everyone, welcome SwiftKey to Windows 10! Back in 2016, Microsoft purchased the SwiftKey keyboard. SwiftKey is a touch screen keyboard that allows for swipe styling typing. Not impressive on its own, the SwiftKeyboard boasts that it has more accurate autocorrect and predictions by learning your writing style. SwiftKey is intriguing, but a feature that, in reality, doesn't change much for most people.

The final big feature, the Windows 10 smart phone integration, is equal parts exciting and scary. Any new sync system has the potential to be attacked, depending on the security in place.

The integration brings you the instant access to your photos from your phone to your PC. There are also plans to add sync notifications in the future. There is also the "Continue on PC" option that will allow you to access a link from your computer, picking up where you left off on your phone.

While there are no earth-shattering changes, the biggest concern is how these updates and changes to Windows 10 will affect you in the long run. As with updates in the past, there is a possibility that any of these new system changes will cause issues with different existing applications and processes. 2017's Fall Creator's update was the culprit behind numerous applications failing, even people having to do full system restores for no real reason.

While the update will be available in early fall, I would suggest avoiding installing the update until you have to. Especially in a business setting. You can try it at home first, but unless you are running the same applications, there is no way of telling how the changes will affect your system until others discover potential issues.

Researchers Turning To Algorithms To Combat Phishing

Chris Myers is a field service technician at Tech Experts.

Phishing is a type of social engineering attack used to steal user information such as login credentials, bank account information, or credit card numbers. The most commonly seen phishing attack is when an attacker, posing as a legitimate source, tricks a victim into clicking on a malicious link in an email. Once clicked, the link installs malware on the user's computer and possibly gives the attacker access to other devices on the same network.

Often, the link opens a website owned by the attacker, specifically designed to look like a normal login or account validation page. However, when users enter their information into this website, all they are doing is giving that information directly to the attacker.

Phishing emails have been around since the dawn of the Internet, even having a paper and presentation discussing their use at the 1987 conference for the International HP Users Group, "Interex."

While the basic premise hasn't changed since then, attackers have had decades to improve their technique and automated delivery systems.

A New Defense

Jeremy Richards of the mobile device security company Lookout has been developing a novel solution to this problem. Lookout records the network traffic of over 60 million mobile applications and, as such, has a large amount of real-time data it can analyze.

After manually tracking phishing websites through this network, Richards discovered many telltale digital signs of phishing websites. He started creating tools to assist in this detection, but those quickly evolved into their own automated search engine.

The program now goes through several steps to algorithmically narrow down and positively identify malicious websites. For example, the program will check new domains (website addresses) for misspellings of technology or financial companies, or special characters used in place of normal lettering.

Once it spots a suspicious website, it will take a screenshot of the homepage and then automatically search for the logos of thousands of companies. Phishing websites almost always try to look official by using the actual logos from companies like Apple, Microsoft, and Google.

Once a site is confirmed to be malicious, Lookout can report them to the authorities, download the specific phishing code used by the attackers, then look for that code in future scans to find additional websites.

As phishing attacks occur with increasing frequency, these automated solutions will be necessary for us to stand any chance at stemming the tide of cybercrime.

How To Spot Phishing Emails

Here are some common characteristics of phishing emails that you can identify:

Poor grammar - Since most emails aren't composed by native English speakers, they usually contain many grammar, spelling, and capitalization mistakes, along with unusual phrasing.

Generic or informal greetings - If a message doesn't address you by name, it's another sign that it is from an unknown attacker.

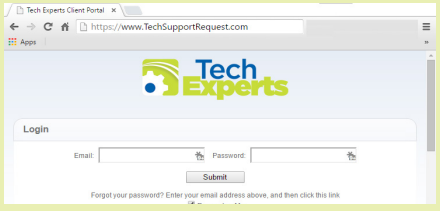
Sense of urgency - Most phishing emails want you to rush through the message and click on a link without looking at it too closely.

Hyperlinks - Hover over any links to make sure they go where they say they are going.

Attachments - Many phishing emails will include malware in attachments.

Unusual sender - If it's from someone you don't know, pay extra attention to the contents.

"Phishing emails have been around since the dawn of the Internet, even having a paper and presentation discussing their use at the 1987 conference for the International HP Users Group, 'Interex.'"



Create new service requests, check ticket status, and review invoices in our client portal:
http://TechSupportRequest.com

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(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) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

How Much RAM Does Your PC Really Need?

Frank Deluca is a field service technician at Tech Experts.

First off, note that how much RAM (along with the type and speed) that your system supports will depend on your motherboard.

Consult your PC/motherboard manual, or, if your PC was manufactured by an OEM, use a system checker such as the one found on Crucial.com to find out what RAM is compatible with your system.

Adding RAM to your computer is not a process that will magically make everything run faster. But it can aid your PC in multitasking and performing intensive-heavy tasks like loading 20+ browser tabs, content creation like editing videos or images, editing multiple productivity documents, and running more programs at one time.

Computers may experience significant slowdowns when running a large number of programs at once with low memory.

If all RAM space has been used when trying to open programs, the computer resorts to using virtual memory on the hard drive, which slows the computer down quite a bit.

Upgrading or adding additional memory can eliminate this problem as the computer doesn't have to resort to using the hard drive for slower pagefile memory.

How much RAM you need in your computer depends heavily on what you use your PC for on a day-to-day basis and on how long you intend to keep the computer.

If you are thinking of investing in a new machine in the near future, waiting things out until your purchase might be the best bet.

If you already have a computer you love but want to shift gears into a different daily task that requires better performance, then upgrading your RAM as part of the process is a great idea and can breathe some extra life into your computer.

Productivity

If you use your Windows 10 computer for word processing, checking emails, browsing the Internet, and playing Solitaire, you should have no problem using 4GB of RAM. If you are performing all of these activities at once, however, you might experience a dip in performance.

Many budget PCs come with 4GB of RAM as a base option. If you plan on keeping your machine for several years, then opting for 8GB of RAM is the safer bet, even if you use it for light tasks.

Video and Photo Editing

This really depends on your workload. If you are editing quite a bit of HD video, go for 16GB or more. If you're working mainly with photos and a bit of video thrown in, 8GB should get you through. Again, in this instance, it may behoove you to opt for 16GB to give yourself more future-proofing headroom as photo and video quality is only getting better with file sizes exponentially increasing and becoming more memory intensive. Editing will work on lower amounts of RAM, but you'll become so frustrated with the poor performance that you'll soon start yearning for an upgrade.

In a nutshell, here are some simple guidelines that apply to most PC devices:

- 4GB: Entry level memory. Comes with budget notebooks. Fine for Windows.
- 8GB: Excellent for Windows and Mac OS systems. We recommend this for most people.
- 16GB: Ideal for professional work and the most demanding tasks.
- 32GB and beyond: Enthusiasts and purpose-built workstations only.

Remember, buying more RAM than you need doesn't net you any performance benefit. It's effectively wasted money.

Buy what you need, and spend what's left of your budget on more important components such as the CPU or faster storage space like a solid state hard drive (SSD) which can be 10 times faster than a conventional hard drive.