E-NEWS

June 2018

In this issue…

Virtualization isn't as complex as you think

Explaining the concept of virtualization is no easy task, and failed attempts to do so have left it with an undeserved reputation. We want to set the record straight about this technology's many benefits by dispelling the four most common misconceptions.

Myth #1 - Virtualization is too expensive for SMBs

Many people assume that the more advanced an IT solution is, the more expensive it is to install and maintain. That's not the case for virtualization, which is a strategy to boost hardware efficiency and *cut costs*.

Sure, a virtual server requires more support than a traditional one, but the capacity boost means you won't need to purchase a second server for a long time -- resulting in a net reduction of hardware and IT support expenses. Furthermore, managed virtualization services usually follow a pay-as-you-go model that costs just a few bucks per hour.

Myth #2 - Virtualization adds workplace complexity

Most people feel comfortable with the traditional computing model -- one set of hardware equals one computer -- but that doesn't mean a new model has to be more complicated. With virtualization, one "traditional" computer can run as two or more virtual computers. The technical aspects of how that's accomplished may be confusing, but the good thing is business owners don't need to bother with those details.

Virtualization actually *reduces complexity* because it allows business owners to expand their IT systems whenever necessary without having to worry about hardware limitations

Myth #3 - Support is hard to come by or inconvenient

You may be more familiar with The Cloud than with virtualization, but that doesn't mean the latter is a niche technology.

The value of the virtualization market in 2016 was $5.6 billion and supported by IT providers all over the country. It's also a technology that works well with remote support, which means technicians can install upgrades or resolve issues without having to travel to your office.

Myth #4 - Software licensing is more difficult

There's a misconception that if your server is running three virtual Windows 10 computers, you'll have to jump through extra licensing hoops. In reality, virtualization follows the same licensing rules as traditional computing: one desktop, one license, which means you won't need to rethink your software budget.

It's natural for new technologies to cause confusion, and virtualization does require a new way of thinking about IT hardware. But as long as you have certified technicians like ours on hand, everything will run smoothly. Give us a call today to find out how we can lower your hardware costs and simplify your IT support.

Little-known Windows 10 tips and tricks!

Are you making the most out of your Windows 10 computer? If you haven't tried adjusting system and battery performance, silenced notifications, or used the night light function, then you're missing out on minor but useful features.

Performance/Power slider

There are two kinds of computer users: those who value battery longevity and those who prefer optimized system performance. The Performance/Power slider in Windows 10 lets you easily toggle between the 'Best battery life' (when you're trying to save battery) and the 'Best performance' (when you need your system to perform optimally), or set a balanced battery and system performance setting.

Just click the battery icon in the taskbar and adjust the slider based on your preference.

Night Light

Those who use computers late at night can turn on Night Light to reduce the amount of blue light emitted from the screen. This feature substitutes the blue light with warmer colors, which reduces eye strain and helps you sleep easily.

Night Light is disabled by default, so you need to enable it by following these steps:

- Click the Start Menu
- Click the Settings app (or press WIN + I to quickly open Settings)
- Click the System icon>Display
  Set Night light to 'On' or 'Off'

Taskbar pin

It takes only a few seconds to open a browser and type a website's address or click Bookmarks and choose from a list of websites you frequently visit. But Windows 10 offers an even quicker way to access your go-to sites by allowing you to pin websites on the Windows 10 taskbar.

Simply click "Pin this page to the taskbar" on the Microsoft Edge menu, and the site's icon will appear on the taskbar for easy perusal.

Drag to pin windows

Need to organize your screen but can't help having many open windows? Reduce screen clutter by dragging any window to a corner so it can take a quarter of the screen. For multiple screens, drag a window to any border and wait for the prompt that tells you to put the window in the selected corner.

Focus Assist

Notifications can be distracting, but Windows 10's Focus Assist feature can manage the notifications you receive from contacts and applications. This function also lets you customize the list of notifications you wish to prioritize.

To enable Focus Assist, go to:

- Settings
- System
- Focus Assist
- Adjust the notifications settings

based on your preference
If you wish to disable it and receive all

How to defend against insider threats

First off, what is an insider threat in healthcare? An insider threat is an individual inside an organization discovered to have been accessing healthcare records without authorization. Healthcare companies must take steps to reduce the potential for insider threats, which is their top source of security incidents.

#1 Educate - The workforce (meaning all healthcare employees) must be educated on allowable uses and disclosures of protected health information (PHI) and the risk associated with certain behaviors, patient privacy, and data security. For example, when a celebrity is admitted to hospital, employees may be tempted, just out of curiosity, to sneak a look at their medical records, so this must be emphasized as a definite no-no.

#2 Deter - Policies must be developed to reduce risk and those policies must be strictly enforced. The repercussions of HIPAA violations and privacy breaches should be clearly explained to employees. They can be penalized huge amounts of money and violations can also carry criminal charges that can result in jail time.

#3 Detect - Healthcare organizations should implement technology to identify breaches rapidly and user-access logs should be checked regularly. Organizations need to have a strong audit process and ensure that they are regularly monitoring and updating access controls so only authorized personnel are looking at sensitive patient data, and that attempts by unauthorized personnel don't go unpunished.

#4 Investigate - When potential privacy and security breaches are detected, they must be investigated promptly to limit the damages. When the cause of the breach is identified, steps should be taken to prevent recurrence.

#5 Train - Healthcare employees must undergo regular comprehensive training so employers can eliminate insider threats. From a privacy standpoint, training and education often start with the employees themselves; they learn all about data privacy right off the bat, from the first day of orientation. Still, organizations must remain vigilant and ensure that they are properly prioritizing privacy and security as cybersecurity threats continue to evolve. Healthcare organizations' IT departments should send out different tips covering a variety of topics regularly throughout the year. And to keep these tips top-of-mind among employees, IT departments should send them via a variety of media, including emails, printed newsletters, and even memos.

Is your healthcare data secure? What other steps can you take to ensure protection for your healthcare provider from insider threats? Call today for a quick chat with one of our experts for more information.

Refer to Win!

Referrals play a big role in our journey to help the many businesses that we do with their IT support. To show our appreciation for all of the kind words and new business you provide, we want to give you a chance to win TWO TICKETS TO A PIRATES GAME
All you have to do is refer one person who agrees to meet with us and we will put your name into a drawing to win . We'll also send the people that you refer who meet with us a voucher entitling them to (2) FREE HOURS of computer support so everyone wins!!!

Malware hits 500k IoT devices, Talos Reports

A week ago, leading cyber threat intelligence team Cisco Talos reported that no less than 500,000 IoT devices in up to 54 countries were infected by new malware called VPN-Filter. An earlier version, believed to be launched by a nation-state, targeted Ukraine.

How VPNFilter Works

Talos cited the vulnerable devices as Linksys, MikroTik, Netgear, and TP-Link networking equipment, as well as network-attached storage (NAS). Upon infecting a small office home office (SOHO) router, VPNFilter deploys in three stages.

In stage 1, the malware imposes its presence by using multiple command-and-control (C2) infrastructure to capture the IP address of the existing stage 2 deployment server. This makes VPNFilter so robust that it can deal with any unpredictable changes in C2. This stage of the malware persists through a reboot, which makes preventing reinfection tough in stage 2.

Stage 2 involves deploying modules capable of command execution, and data collection and exfiltration. According to the United States Department of Justice (DOJ), this can be used for intelligence gathering, information theft, and destructive or disruptive attacks. Moreover, stage 2 malware has a "self-destruct" feature that once activated by the hackers will overwrite a critical area of the device's firmware so it stops functioning. This can happen on almost every infected device.

In Stage 3, a module with packet-sniffing capabilities is added to enable monitoring of internet traffic and theft of website credentials. And yet another module is installed to deploy communication support for the Tor network, which can make communicating with the C2 infrastructure harder.

Taking Action

According to Talos, the likelihood of the attack being state-sponsored is high, something the DOJ later backed up. The DOJ attributed it to a group of actors called Sofacy (also known as APT28 and Fancy Bear), the Kremlin-linked threat group believed to be responsible for hacking the Democratic National Committee computer network two years ago.

On the night of May 23, the FBI announced that they have seized a domain which is part of VPNFilter's C2 infrastructure used to escalate the malware's effects. This forces attackers to utilize more labor-intensive ways of reinfecting devices following a reboot. With the seizure, the government has taken a crucial step in mitigating VPNFilter's impact.

Stopping the Malware

Researchers agree that VPNfilter is hard to prevent. While vulnerability has been established, patching routers isn't easy, something average users might not be able to do on their own. But as with any malware, the impact of VPNFilter can be mitigated, which is done by terminating the C2 infrastructure used.

To minimize exposure, the FBI recommends all SOHO routers be rebooted, which, according to a statement from the DOJ, will help the government remediate the infection worldwide. The justice department, along with the FBI and other agencies vowed to intensify efforts in disrupting the threat and expose the perpetrators.

For their part, Talos offers the following recommendations:

- Users of SOHO routers and/or NAS devices must reset them to factory defaults and reboot them in order to remove the potentially destructive, non-persistent stage 2 and stage 3 malware.
- Internet service providers that provide SOHO routers to their users should reboot the routers on their customers' behalf.
- If you have any of the devices known or suspected to be affected by this threat, it is extremely important that you work with the manufacturer to ensure that your device is up to date with the latest patch versions. If not, you should apply the updated patches immediately.
- ISPs will work aggressively with their customers to ensure their devices are patched to the most recent firmware/software versions.

Combat the VPNFilter malware by rebooting affected devices. For more tips, contact our team.