E-NEWS

www.E-Safetech.om | 1-412-944-2402 |

March 2017

In this issue…

What Exactly is Preventive Cyber–Security?

There has been a movement among technology providers to promise "proactive" cyber security consulting. Small- and medium-sized businesses love the idea of preventing cyber-attacks and data breaches *before* they happen, and service providers would much rather brainstorm safeguards than troubleshoot time-sensitive downtime events. But it's not always clear what *proactive cyber-security* means, so let's take a minute to go over it.

Understand the threats you're facing

Before any small- or medium-sized business can work toward preventing cyber-attacks, everyone involved needs to know exactly what they're fighting against. Whether you're working with in-house IT staff or an outsourced provider, you should review what types of attack vectors are most common in your industry. Ideally, your team would do this a few times a year.

Reevaluate what it is you're protecting

Now that you have a list of the biggest threats to your organization, you need to take stock of how each one threatens the various cogs of your network. Map out every device that connects to the internet, what services are currently protecting those devices, and what type of data they have access to (regulated, mission-critical, low-importance, etc.).

Create a baseline of protection

By reviewing current trends in the cyber-security field, alongside an audit of your current technology framework, you can begin to get a clearer picture of how you want to prioritize your preventative measure versus your reactive measures. Before you can start improving your cyber-security approach, you need to know where the baseline is. Create a handful of real-life scenarios and simulate them on your network. Network penetration testing from trustworthy IT professionals will help pinpoint strengths and weaknesses in your current framework.

Finalize a plan

All these pieces will complete the puzzle of what your new strategies need to be. With an experienced technology consultant onboard for the entire process, you can easily parse the results of your simulation into a multi-pronged approach to becoming more proactive:

- Security awareness seminars that coach everyone -- from receptionists to CEOs -- about password management and mobile device usage.
- "Front-line" defenses like intrusion prevention systems and hardware firewalls that scrutinize everything trying to sneak its way in through the front door or your network.
- Routine checkups for software updates, licenses, and patches to minimize the chance of leaving a backdoor to your network open.
- Web-filtering services that blacklist dangerous and inappropriate sites for anyone on your network.
- Antivirus software that specializes in the threats most common to your industry.

As soon as you focus on *preventing* downtime events instead of *reacting* to them, your technology will begin to increase your productivity and efficiency to levels you've never dreamed of. Start enhancing your cyber-security by giving us a call for a demonstration.

March Madness 2017 Recap

The biggest event of the year was a blast!

It's March and you know what that means,.. March Madness! This year we were excited to host our customer appreciation event at the Hard Rock Café located at Station Square in Pittsburgh. The day was filled with basketball, food, technology, gifts, GREEN beer, and Pittsburgh Dad!

This years event was all about the latest products and solutions in the IT industry from leading technology vendors. Vendors in attendance this year were: Black Box, Kaminario, Barracuda, Data Gravity, Exagrid, Sophos, PacketViper, Citrix, Datto, and Veeam. We'd like to give a big thanks to them all for helping make this event possible this year.

The vendors presented on the most relevant subjects in technology and covered important topics such as Global Threat Intelligence, Backup and Disaster Recovery, Virtualization Monitoring, Managed IT Services, All -Flash and Hybrid Storage Solutions On Demand. If you missed this event, you missed out on some great information. That's ok though, our vendors gave us the powerpoints to their presentations that can be found at www.E-SAFETECH.com/resources/march-madness-presentations/

The team at E-Safe wants to thank everyone in attendance for coming out and spending a fun filled day with us. Without our wonderful customers, this day would not have been possible and for that we thank you.

If you have any questions about the event and information that was presented, please feel free to reach out to us! We would love to hear from you and talk about the exciting new things are vendors are bringing this year.

Windows 10 FREE Upgrade for SMB's

Microsoft has announced that it will bring back free Windows 10 upgrades, but on one condition: Only small- and medium-sized businesses that have previously passed on the offer are eligible. So if you or someone you know has declined Microsoft's previous proposition, here are some reasons you might want to reconsider.

"*They're extending the free upgrade to this segment of customers to help them get to Windows 10,*" said Wes Miller, an analyst at Direction on Microsoft, specializing in complex licensing rules and practices. Much like the 12-month upgrade deal that ended last August, this offer applies to personal computers running on Windows 7 or Windows 8.1. The only difference is, the offer is exclusive for businesses that have subscribed to one of the Windows Enterprise plans.

According to Nic Fillingham, a small business product manager: "*Customers subscribed to Windows 10 Enterprise E3 and E5 as well as Secure Productive Enterprise E3 and E5, can now upgrade their Windows 7 and Windows 8.1 PCs and devices to Windows 10 without the need to purchase separate upgrade licenses.*"

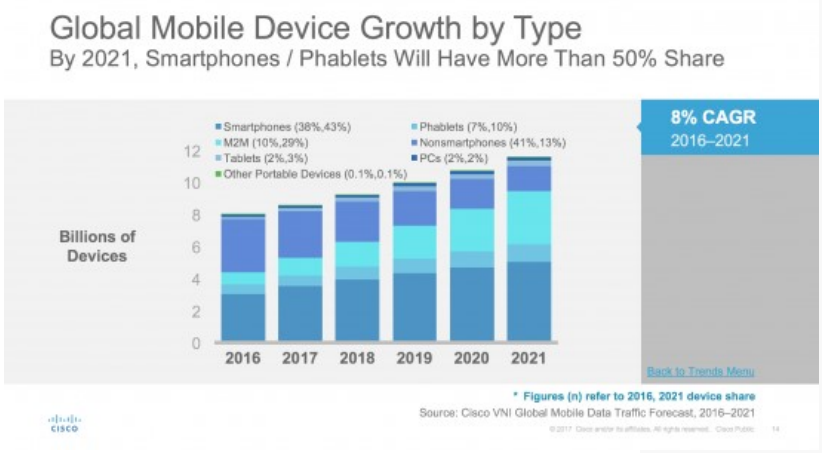
The Windows 10 Enterprise E3 and E5 subscriptions are priced at $7 per user per month and $14 per user per month, or $84 and $168 per user annually. Unlike Microsoft's historical licensing -- which permanently licensed the operating system on a per-device basis -- the E3 and E5 subscriptions are per-user licenses, and payments must be maintained to run the OS. This was introduced to target customers that didn't want to sign a long-term volume licensing agreement.

In order to qualify for a Windows 10 Enterprise E3 or E5 subscription -- which are delivered through a CSP (cloud service provider) -- devices must already be running on Windows 10 Pro. SMBs could upgrade their devices for free last year if those devices ran older Windows 10 versions, and SMBs can upgrade the devices they newly acquire this year if those devices are already equipped with Windows 10 Pro.

Give us a call to find out more today!

IPv6 Enables Global Mobile IoT Innovation and Profileration

Digitization and automation is now a familiar feature in many homes. Mobile connectivity is not just for phones anymore. Today, we have lots of things that generate data or environments that we want to control (locally or remotely). And our access point for control is not limited to our smartphones – televisions, tablets, smartwatches, health monitors and even kitchen appliances can all serve as "digital control points." Ubiquitous connectivity and control are fundamental elements of the Internet of Things (IoT) value proposition. The challenge of delivering seamless user experiences through communications between all of our devices and things that we want to control is becoming more broad and complex. According to the 2017 Cisco Mobile Visual Networking Index (VNI), there will be nearly 12 billion global mobile-connected devices and machine-to-machine (M2M) connections by 2021, approximately 1.5 per capita. Globally, mobile networks will support about 4 billion new mobile-connected devices and connections from 2016 to 2021.



The chart above indicates that nearly a third of all mobile devices and connections (about 3.3 billion) will be some form of M2M by 2021, However, the full vision and potential of IoT can only be realized if **real-time information** is transmitted **securely** to a **wide variety of users and things**. IPv6 is a key enabling component of of this aspirational networking goal. Service providers around the world understand the fundamental importance of IPv6 and the inherent innovation possibilities that it it can unlock. Service Providers like Comcast see IPv6 as much more than just a more scalable addressing scheme. The Cisco Mobile Visual Networking Index (VNI) forecasts that globally, there will be 8.4 Billion IPv6-capable devices/connections by 2021, up from 3.4 Billion in 2016. Here's specifically how IPv6 addresses the three primary characteristics for successful IoT growth:

> *"The interesting thing with IPv6 is that we're going to rethink how address space is used," said Kevin McElearney, SVP of network engineering for Comcast. "Right now, everybody thinks that IP addresses are devices, but if the Internet of Things is really the Internet of virtual things then every device could have 100 or 1,000 addresses so it's going to get interesting if you want to start addressing things like blocks of storage, application calls, or services."*

Real time information: One of the key metrics to evaluate the quality of information is whether it can be acted upon in a timely fashion. 'Real time actionable information' can be life-saving, be it the multitude of wearable health monitoring devices monitoring a patient's health vitals or communication devices that enable pilot and air-traffic control communication. IPv6 enables faster communication by eliminating significant administrative overhead that exists in the IPv4 networks today – faster packet processing through elimination of IP checksums, faster routing through elimination of multi-layered routing and shorter routing tables and bandwidth efficiency through multi-casting in place of broadcasting, to name a few.

Security: While there are significant technological benefits that IPV6 provides in enabling IoT, one of the key benefits is the processing and transport of information in a secure fashion. IPSec, which provides end-to-end confidentiality, authentication and data integrity, is already present in IPv6. What that means is from the point where the data originates to its point of destination the data is secured and encrypted thus reducing cyber attacks where data can be hacked during transit.

User Adoption: With the plethora of devices and things that users are surrounded with, the key component of user adoption is 'ease of setup' and 'ease of use'. Users now expect devices to come without extensive product manuals and work upon first power-on as soon as they remove it from the box. IPv6 offers this 'out of the box' experience through static IP addresses for each device or M2M connection, which eliminates the need for extensive manual configuration to connect new digital devices or things to a network. IPv6 connections can be pre-configured for first-time use, thus enabling and simplifying IoT.

So, even though the initial value of the IPv6 protocol was seen as a solution the acute IP address shortage, we now know that it delivers much more than just scalability. IPv6 can also help service providers build larger, more efficient networks with greater mobile connectivity and interoperability (especially for IoT). These networking transformations can support greater business innovations and revenue generation opportunities for service providers.

Battle of the Robots! (Wiki Style)

“Benevolent bots” that are designed to improve articles on Wkipedia have online “fights” over content that can continue for years, researchers have found.

Software robots, editing bots on Wikipedia undo vandalism, enforce bans, check spelling, create links, and import content automatically. The research paper, published in PLOS ONE, said bots appear to behave differently in culturally distinct online environments but “are more like humans than you might expect.”

It is a warning that to those who use AI for building autonomous vehicles, cyber security systems or for managing social media. Although bots are automation that do not have the capacity for emotions, bot to bot interactions are unpredictable and act in distinctive ways.

Taha Yasseri said: “Bots are designed by humans from different countries. So when they encounter one another, this can lead to online clashes. We see differences in the technology used in the different Wikipedia language editions that create complicated interactions. This complexity is a fundamental feature that needs to be considered in any conversation related to automation and artificial intelligence.”

WordPress Vulnerabilities

“Easy-to-use,” “SEO-friendly,” “open-source,” and “customizable.” These are some of the words that best describe WordPress, currently the most popular Content Management Solutions (CMS) platform. With thousands of websites affected in a recently launched series of attacks, “easy to target,” “hackers’ favorite,” and “prone to attacks” could soon be used to define the experience of running a WordPress website.

WordPress attacks by the numbers

In 4 separate attacks, an estimated 40,000 websites were compromised, defacing 67,000 web pages, which has quickly gone up to 1.5 million. A security release update, WordPress 4.7.2, was immediately launched to mitigate the flaw, but not everyone was able to deploy it on time, thus inflating the number of corrupted web pages.

Although WordPress took measures to ensure that the vulnerability would go unnoticed, hackers found a way to get around the initial fixes and exploited the sites that remained unpatched. Those who haven’t applied WordPress’s latest security release were the ones most harmed by the defacement campaigns, and it soon became highly publicized.

Steps taken

Fixes have been deployed and stronger patches are in the works, but hackers do not just sit around and wait to be taken down. In fact, more attacks are being launched concurrently with security developers’ attempts to strengthen blocking rules.

In preparation for further exploits, WordPress liaised with cybersecurity firms to implement protective measures. Google did their part by announcing via Google Search Console the critical security updates that webmasters must install to protect against the WordPress-specific attacks. Meanwhile, web application vendors and web hosting companies are poised to protect their customers from attacks by installing web filters on their customers’ web servers.

Despite these measures, the attacks are expected to continue and the masterminds behind them will come up with strategies more insidious than merely modifying several web pages. Updating security patches that can effectively alleviate the vulnerabilities’ impact will also take time to develop and launch.

The importance of patches

Some attacks may cause a blip on your business’s networks, while others might cause its demise. From all these attacks, one lesson is worth emphasizing: Applying the most up-to-date patches is critical to your systems’ security and business’s survival.

Unpatched systems are the easiest targets for hackers who are always on the lookout for vulnerabilities to exploit. If your organization lacks the capacity to manually update security patches, consider deploying patch management software. Keeping all your software updated with the latest patches may seem like an insurmountable task, but the price of neglecting it can cost you dearly.

WordPress remains the most widely used CMS and its popularity is not going to wane anytime soon. If your website runs on WordPress and you’re considering security options that will ensure your company is poised to handle breaches, contact us for advice.