Happy Halloween!

October 2019

microTECH Times

Covered I.T. 24/7—Never Worry Again!

How Patch Management Can Save You From A Frightening IT Security Breach

Have you heard of Equifax? Yes, the major credit reporting agency. According to Wired, their security was compromised in mid-May when there was a patch available in March for the vulnerability that caused all the trouble. Read on to learn how proper patch management can save you from a terrifying IT security breach like this.

What is patching? Patches are a set of changes or updates for a computer program or its supporting data that is developed to improve or fix a troublesome area that may lead to an attack. Patches, also called bugfixes, close security loopholes improving the performance and functionality of the program.

Why is patching so important? Hackers just love security flaws. They flock to software users that have programs riddled with open vulnerabilities. Software companies work tirelessly to assess their software and ensure their clients are protected. However, if the patches the software companies release to repair their products are never applied, guess what? You're left unprotected!

I know it's tempting to just click, "Remind me later" when the notification shows up on your computer. Don't do it! Take time to update your software immediately to avoid leaving a vulnerability open on your network.

Make patching a top priority. Even in just two short months, attackers were able to pinpoint the weakness at Equifax and exploit their system. Wired reported that over 147 million people were exposed from this blunder. This type of breach sure shows why patching should be a top priority for all companies. Just 60 short days allowed hackers to wiggle in the through the vulnerabilities. Imagine how quickly they will stride right into your network. So, how can you actively manage these scary cyber security threats?

(Continued on page 2)

What's Inside

Cursed Courser?

Has your courser been moving on it's own? Here are some quick fixes to consider:

1. Check the hardware on your mouse for debris and clean it.
2. Change the touchpad delay.
3. Disable the touchpad.
4. Update your mouse driver.
5. Run the Hardware and Devices troubleshooter.
6. Check for Malware.
7. Disable Realtek HD Audio manager.
8. Update Windows.
9. Change your mouse sensitivity.

Happy Halloween!

According to the History channel, Halloween originated with the ancient Celtic festival of Samhain. Take a look at the true history of Halloween and share the story with your family, friends and coworkers too.

What is Samhain?
It is an ancient Celtic festival celebrated over 2,000 years ago with bonfires and costumes to ward off evil ghosts returning to earth. The Celtic's believed the night before the new year was when the veil between living and dead became blurred. Samhain was also a time to celebrate the new year being the end of summer and the beginning of the harvest season. This is the first recorded celebration that mimics Halloween today.

Pope Gregory III…
dubbed November 1st as a time to honor all saints. Soon, All Saints Day incorporated some of the old Samhain traditions and the evening before became All Hallows Eve. Many people would gather to honor the dead, join in pa-

(Continued on page 3)

microenterprises

**234 N Broadway Ste 2,
Pennsville, NJ 08070**

**877-540-6789
www.microent.net**

How Patch Management Can Save You…

(Continued from page 1)

Appoint a person to manage patching. Patching isn't rocket science, but it is often overlooked. Some companies have a handful of people internally that take on the responsibility and hope they get all the systems updated with all the patches needed. However, the full process of patching all necessary systems never seems to be owned by any one person. This often leads to confusion and finger pointing when something is missed or infected. Be sure to appoint one individual to handle all your patching to ensure it is done in a timely manner, complete and issues are resolved quickly.

Don't accept rotten results. Implement testing procedures after the patches are installed so you can say with 100% certainty that your company is up-to-date and working properly. Some patches may break connections in your network. Protect your company from these pitfalls by walking through all the trial and verification steps necessary to head off adverse consequences.

"I've changed. Now I only release the flying monkeys when I'm out of coffee."

Analyze and follow-up. As with anything IT related, it's important to analyze Your patching procedures. Closely monitor and document patches released from vendors, when they were tested, deployed and completed. Managing this type of information can be a daunting task. We recommend a system or dashboard to streamline how the data is collected, stored and recalled. This will give all parties involved a clear picture of the entire patching initiative. Should there be an incident, this type of data will assist IT professionals in understanding where the vulnerability may have been and if there are additional vulnerabilities to address.

Sweet intentions and sour results. No one really loves patching. Really, that is not a thing. Even in the IT world we don't sit around and fight over the patch management duties for our clients. However, due to its importance, we do make it a top priority and quadruple check to be sure there are no open doors for goblins to flood your network. The truth… patching is an essential part of technology in business. It not only updates your software programs or operating systems but in turn protects your data too.

Cyber security is all about you! Just like the flu, a computer virus can spread between your devices, into your home computer, and of course, your computer network at the office. Develop healthy computing habits. Put a trusted security program and an offsite back-up solution in addition to implementing proper patch management.

Need help? Don't hesitate to give us a call. We offer a full patch management solution with out managed service packages. We will make sure all your computers and programs are always updated and patched in a timely manner.

What NOT To Do After A Breach

Has your security been breached? Here's a few pointers of what NOT to do.

1. Do NOT improvise. Your company deserves the best. In the event of an attack you may be tempted to try and fix things yourself on the fly. The last thing you need is to waste time trying to organize a recovery plan. Be proactive about your IT management. Put a back-up and recovery plan in place today so everyone knows exactly how to respond if there is a breach.

2. Do NOT be silent. Communicate with your staff, customers and vendors to ensure everyone knows what's been accessed and how you plan to remedy the situation. If you don't there are a mound of risks that really aren't worth the reward.

3. Do NOT close the case to soon. You've closed the corrupted endpoints and informed everyone of the issue at hand, recovered your data and you're back to business as usual. It's time to close the logs for the attack, right? Wrong. Be sure to investigate the root cause and review your network after you've remediated to identify any additional weaknesses the attacker may have opened up.

Happy Halloween...

(Continued from page 1)

rades, and dress as angels, saints, or devils.

True Halloween in America. Even at the start of the 19th century, Halloween as we know it today still wasn't really a thing. Colonial Halloween festivities included things like story telling, food, and dancing. However, in the second half of the century, America was flooded with new immigrants, namely millions of Irish fleeing the Potato Famine, who celebrated All Saints Day.

Blame it on the Irish. The influx of Irish natives helped popularize the celebration of Halloween nationally. Borrowing some old traditions from Europeans and starting some new ones of their own, American's began the tradition of trick-or-treating. They would dress up in costumes and go house to house asking for food or money. In the late 1800's, the holiday really started to flourish into what we know today.

Celebrate safely. Today, Halloween parties with young and old alike are celebrated across our nation. Games, foods of the season and festive costumes are shared by all. Be safe this Halloween and enjoy the festivities.

Why Does Your Greasy, Grimy, Bacteria Ridden Hardware Need To Be Cleaned?

Having to worry about hardware issues in your business can be frustrating and cost you precious time as well as money. Dust, dirt and grime can bog down your equipment. Take a look at these tips to keep your hardware clean and in good working order.

Greasy fingers lead to grimy keyboards. We've all done it; grabbed a quick bite to eat at our desks while we continue working on critical work. However, those greasy fingers from that yummy slice of pizza or panini sandwich can leave your keyboard a grimy bacteria ridden mess. Clean your keyboard often, especially if you eat at your desk. Unplug your keyboard and turn it over a waste bin to shake any crumbs or debris out. Then use a damp cloth with a disinfectant cleaner sprayed on it or a wet wipe of sorts to clean oils or bacteria from the keys.

Don't let your mouse skip out on a good cleaning too. Your mouse is under your hand all day. Anything you touch will be transferred to your mouse and mouse pad. Most mouse pads can withstand a good scrubbing in the sink with antibacterial soap, just be sure to let it fully dry before putting it back in place. Your mouse requires a little more attention. Pesky buildup can form on the surface and underneath as well. Start by unplugging your mouse from your computer and/or remove the batteries. Use a clean cloth with a bit of alcohol to wipe down the outside and the sensor underneath. If you have a mechanical mouse, place it on a piece of plain white printer paper and tap it down as well as roll it around to clear excess debris.

Dust balls bearing down on your fan. Cleaning the outside of your computers is a wonderful start but, don't forget about the inside too. We recommend popping open the case on your tower computer at least two times a year to clean out the inside too. Dust balls can build up inside causing the fan to slow or seize. Be sure to use a static free vacuum to remove dirt and dust buildup inside or blow it out with a can of compressed air.

I can see clearly now the dirt is gone. You'll be surprised at how dirty your monitors can get. You can use glass cleaner on a cloth or paper towel to dust off the back and top as well as gently remove excess grime from your screens. Now that your hardware is clean, don't forget the surface of your desk too.

New Authentication Methods Coming Soon That May Freak You Out A Little Bit!

I remember as a small child, watching Star Trek and thinking, "Wow, technology is so cool! They can just waive their hands and open doors or turn things on. I can't wait to see that happen in real life." Well, we are on the verge.

Hitachi Europe is poised to release hand gesture authentication. Hitachi has been a leader in developing new biometric technology methods to replace passwords and authorize transactions. They've developed a new finger vein biometric authentication program so devices with cameras can now scan your hand.

How does it work? Similar to fingerprint technology that scans your fingers for ridges (forming a fingerprint), Hitashi's new method scans your fingers but on the inside. According to the General Manager at Hitachi in a recent Forbes article, finger vein technology reads patterns inside your fingers using ambient or infrared light to see the patterns. The best part is that this new authentication method uses the existing camera on your laptop or smartphone. There is no need for additional sensors or hardware.

The wave of the future. While finger prints are fairly easy to replicate, vein patters are nearly impossible. Developers are even putting several security methods in place to further reduce the instances of fake hands.

Google Calendar Tips

As you review your Google Calendar, you suddenly notice that -- surprise -- you have won a free iPhone X! Yeah, spam is now hitting Google Calendar, be aware of the danger.

Naturally, you know nothing is free and who knows what is at the end of this 'calendar invitation.'

This is what Security expert Graham Cluley calls a scammer desperation move: Calendar invitations.

You can stop them. Go to the gear icon the top right of your calendar screen. Choose settings.

From the drop down menu select Event Settings.

Change the Automatically Add Invitations setting to: No, only show invitations to which I have responded.

Now when someone emails an invitation, you have to respond and then the invitation will be added to your calendar.

"We make all of your computer problems go away without adding additional full-time I.T. staff!"

Ask about our fixed price service agreements — Computer support at a flat monthly fee you can budget for, just like payroll!

Inquiring Minds...

The Deep And Dark Web: What You Should Know. The deep web and dark web are two dramatically different things even though they are related. Here are a few things to consider to keep your information safe online.

What is the deep web? The deep web is a part of the World Wide Web that holds content that doesn't have a permanent URL. This means it is behind a paywall, password protected or dynamically generated. The deep web is not easily searchable by regular search engines. In general, it's a fairly safe place as apposed to the dark web. Did you know that about 90% of the content online is actually blocked from standard search engines because it requires a user name and password for access? There are a bundle of things you probably visit daily that are housed in the deep web like your e-mail account, social media, online banking websites, legal documents, and medical records. A lot of items in the deep web contain information that you really wouldn't want to show up in a Google search because it is private and could be used to hurt you or your business.

What is the dark web? The dark web is actually a little piece of the deep web but, operates with a high degree of anonymity. The dark web is saturated with activities both harmless and criminal. The dark web is just as it sounds; it holds dark content or disturbing illegal content. You can readily find things like stolen information, disturbing services, as well as illicit substances or illegal items for sale.

How to keep your information safe online. Don't trust Internet connections you don't know. Using public Wi-Fi is convenient but, can be a huge risk for your company and personal data. Coffee shops, malls, restaurants, hotels and airports make no guarantee about their Internet connections. As a matter of fact, they generally have you agree to specific terms of use releasing them of all liability for your browsing experience. The security on these networks is extremely lax or may even be nonexistent. Hotspots are a common place for Man-in-the Middle (MitM) attacks, snooping, and spoofing. MitM is when someone is eavesdropping on your activities and intercepting your information. Snooping or sniffing is exactly as the name presents it; a person tagging along with you using special software to capture everything you see on your computer. Other criminals will simply spoof the Wi-Fi connection all together changing one little detail about the connection name. Hotels are a notorious for these types of fake hotspots. You may see something like Hilton_Guest and then you may see, HiltonGuest1. Be sure to check with the business you are visiting to ensure you're on their true connection if you must use a hotspot.

Use encryption to mask your information online. This is the easiest and most effective method to make your data unreadable. Did you know that most routers come with the ability to encrypt data but, it's not turned on by default? Make sure your regular Internet connections have encryption enabled to stay safe.

Tired Of Corny Computer Conundrums Crushing Your Workday?

No tricks, we just want to treat you right. If you're tired of corny computer conundrums crushing your workday, give us a call. We can run a full Network Security Assessment to identify and remedy any computer or network troubles you may have.

Give us a call today to schedule your Network Security Assessment!

Micro Enterprises LLC 877-540 -6789

microenterprises

234 N Broadway Ste 2,
Pennsylle, NJ 08070

877-540-6789
www.microent.net