PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions March 2019

End of Life for Windows Server and Windows 7

Did you know that Microsoft will no longer be offering support for Windows 7 and Windows Server 2008 after January 2020? This means that all security updates will no longer be offered and support will not be provided after this date.

Make plans soon! Contact us at (561)969-1616 for more information and we will ensure that the upgrade runs smoothly!

This monthly publication provided courtesy of Chuck Poole, President of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

The #1 Mistake Your Employees Are Making Today That Lets Cybercriminals Into Your Network

In the wake of unprecedented rates of digital crime, with the cost and frequency of data breaches constantly skyrocketing year after year, companies all over the world have been forced to scramble for solutions. There's an arms race running behind the scenes of every piece of technology we use in business today, as cyber security companies shore up their clients' defenses against increasingly sophisticated digital threats. Billions of dollars are now poured into batting away would-be intruders from the most precious assets on global networks: most of the money directed toward the software that keeps everything afloat, just out of reach of the bad guys.

But even as each day brings a new technological apex for security solutions, data breaches continue. Despite the fact that the tools hackers use to make money are more or less the same as they were three years ago, nobody seems to question why companies are still being hacked at record levels. It's easy to imagine a crack team of infamous hackers hammering away at a keyboard into the late hours of the night, feverishly computing the one piece of code that will break them into a system.

This may be the process behind the high-profile breaches you read about in the news each week, but in reality, most cybercrime takes much less effort. The average hack succeeds not because of overt vulnerabilities in the structure of business networks, but because of a mistake made by you or your employees. According to IBM's X-Force Threat Intelligence Index, more than two-thirds of breaches arise from what

continued on page 2

they call "inadvertent insiders," folks who accidentally left the network vulnerable from one action or another without even realizing it.

Most of the human error that becomes the root cause of catastrophe can be traced back to phishing. A criminal spends some time researching your organization, maybe learning a bit about an employee or two, and decides to masquerade as someone worthy of trust either within your team or from a company you contract with, or just a stock person offering something pretty much everybody wants. They mock up a somewhat convincing e-mail and send it off to 10 people within your business. Somebody clicks the included link without thinking, and there you go – you've got ransomware. If you haven't backed up your data, you're looking at a hefty fee to get everything back, if they even give it back at all.

In other cases, your team may actively duck around your previously implemented security measures or avoid the procedures you've put in place to keep the business safe. That can mean visiting unsavory websites, ignoring a vital security patch or another minor transgression. But when every mistake spells a potentially massive vulnerability, you can't afford people who aren't conducting business to the highest standards in cyber security.

Regardless of how it happens, most hacks occur because employees just don't know better. Even in 2019, when

"Somebody clicks the included link without thinking, and there you go — you've got ransomware."

cybercrime runs rampant and virtually everyone is constantly at risk on the Internet, most of us just aren't well-versed in ways to protect ourselves, much less the companies we work for.

The good news is that this problem is pretty easy to prevent through education. To keep everyone abreast of the latest threats to their livelihood, it takes a thorough set of rules, guidelines and general savvy to steer them through the troubled waters of modern cyberspace.

Of course, this will take more than a 30-minute crash course in the break room one afternoon. It'll take a concerted effort and dedicated resources. Luckily, we can help. With a trusted partner dedicated not only to keeping your organization protected from the latest digital threats, but to keeping your employees alert and ready to spot anything phishy, you drastically decrease the chances of your business becoming another statistic in the war on cybercrime. Work with us and secure the future of your company for the long haul. Call us at **561.969.1616**.

The Creative Curve
by Allen Gannett

According to Allen Gannett, everything we've been taught about creativity is a lie. It isn't only for geniuses, whose inspiration arrives like a bolt of lightning. In fact, Gannett argues, the principles behind achieving success in any creative endeavor, whether it's selling a painting or starting a business from the ground up, is quite predictable.

In his book *The Creative Curve*, Gannett boils down the essentials of creative success into four prime laws. If you've been stuck in a creative rut and are looking to get a leg up on the competition, his book is the perfect place to start.

The Con of Social Engineering: Law Firms Are Easy Prey

A discussion of the threat that social engineering (aka the "human side of hacking") poses to law firms, and some tips and practical guidelines to reduce its effectiveness. What follows is an excerpt:

"The great news is that law firms have readily available steps to dramatically reduce the effectiveness of social engineering ploys and they do not require *Mission Impossible* technology. Social engineering is all about exploiting gaps in humans' knowledge and awareness.

"Law firms investing in cyber social engineering awareness training and regular training of the firm's employees, contractors and even clients will create a powerful first line of defense against this method of attack and remove the bad guys' most effective weapon.

The four top methods of social engineering include phishing (email), vishing (phone), smishing (texting) and impersonation (face-to-face). Each method utilizes unique tactics to create trust and authenticity in the ultimate communication used to defraud the recipient.

The more repetition there is of personalized, detailed or highly focused communications, the higher the rate of success there will be in convincing the recipient to let down her defenses and for her to click on, open or run malignant communications. Combining each of these different methods, and a hacker may even acknowledge in such communication an individual's security training, can produce great results for the hacker.

Training and Testing

Training needs to provide tools to help employees validate the bona fides of the sender of the electronic communication regardless of the method of communication used. Also providing varied examples of how social engineering attacks may occur will get employees thinking outside the standard security box.

Often, attackers play on an individual's weakness, susceptibility and curiosity. The email impersonating someone from human resources or finance with a simple sentence of "Bill, do you really think these expenses should be approved?" with a malicious file attached to it will get hits almost every time.

After monitoring news accounts and press releases and performing other "due diligence" on an unsuspecting employee, such as a company bookkeeper, sending a feigned wire instruction to him just when a transaction is about to close and indicating that payment needs to be made by a certain time for the deal to close often works like a charm to cause payment to be made to the bad guy. Role playing or gaming in employee training will make individuals more aware of their susceptibility to such ruses.

In addition to social engineering training, which is your last line of defense, do not forget to do regular real-world testing. Bring in security professionals, who understand up-to-date social engineering artifices, to challenge your investment in "behavior modification" training of your employees and hopefully validate it and improve your security system.

Empowering your law firm's employees with such cyber fighting skills also can be a huge morale boost transforming them from victims to warriors in the battle to protect confidential client and law firm information. Building a training and awareness environment which seeks to keep this knowledge and awareness fresh, relevant, frequent and varied in its means of delivery will make it effective.

Contact us at 561.969.1616 so we can assist you and your staff stay protected against social engineering threats.

Source: www.law.com

Can You Afford To Lose $80,000 A YEAR? If Not, READ THIS!

According to the Better Business Bureau's 2017 State of Cybersecurity Among Small Businesses In North America report, SMBS lost more than $79,000 to cybercriminals. Honestly, this shouldn't surprise anyone; after all, as even the smallest businesses digitize more and more of their processes, the costs of breaking those systems will continue to skyrocket. If you're a small business owner in 2019, you need to start making cyber security a priority – now. Make a list of clear goals and objectives, and prepare your business for threats coming from all directions, rather than relying on a single defensive strategy that's prone to fail when things get tough.

SmallBizTrends.com, 12/3/2018

End Ransomware With Virtual Disaster Recovery

Ransomware like CryptoLocker and WannaCry has become more sophisticated over the years. No wonder that more ransomware attacks are expected this year. To fend off these threats, turn to virtualized disaster recovery (DR) solutions. They're your best defense against ransomware.

Virtual DR

Virtual DR solutions allow you to create point-in-time copies or "snapshots" of operating systems, data, and virtual machines as they appear at a given point in time. These snapshots can then be loaded onto any workstation with everything still intact. In the event of a ransomware attack, administrators can essentially roll back the system to a point before the malware struck.

What's great about point-in-time copy features is that they are automated. Just schedule the snapshots and your virtual DR software will do the rest. Although virtual DR solutions vary, most of them have the capacity to store thousands of point-in-time copies, giving you plenty of restore points to choose from.

Why virtual DR trumps traditional DR

Most traditional DR methods don't have point-in-time copy features. Even though most computers have a system restore functionality, they can be disabled by newer ransomware strains. On the other hand, virtual DR software isolates point-in-time copies and restores functionality from virtual machines. This means they can't be affected if one virtual machine was compromised with ransomware.

Another reason why traditional DR is not as good of an option is that there is more tedious configuration involved. You have to copy all your data onto a backup drive, reinstall applications, and reconfigure hardware. By the time you've recovered from the ransomware attack, the financial and reputational damage caused by downtime will have taken its toll on your business.

When recovering your system, you want as little hassle as possible. With virtual DR, you can load a clean, ransomware-free snapshot onto your system in less than an hour.

However, implementing virtual DR can be complex, especially if you're not experienced. But if you partner with us, this won't be a problem. Call us today at 561.969.1616 to get robust solutions that guarantee business continuity.

Techadvisory.org

Are Your Credentials For Sale On The Dark Web?

Visit www.palmtech.net/darkweb/ For A Free Scan!