IT Strategy Brief

ISSUE 8 | VOL 6 | August 2020

INTEGRATE SEAMLESSLY

SWK
MANAGED CLOUD SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:

SWK Welcomes Prairie Tech Customers!

SWK is pleased to welcome the Prairie Technology Solutions Group (PT) customers from the Chicagoland area. SWK and PT merged on August 1, 2020 – read the press release here -- to expand our real-time service and support for technology stacks hosted in the cloud or on premises across the Midwest.

SWK is a technology implementation and consulting company that helps you integrate your software and network solutions seamlessly. Along with our extensive ERP and software solutions practice, we're also an award-winning MSP and cloud application hosting provider.

John Eslinger, president of PT, has joined the SWK Strategic Technology Advisory Team (STAT), a complimentary business management consulting service we offer to customers looking to improve ROI on their digital investments.

John and the rest of the PT team will continue to support your organization today and well into the future. Welcome!

Add Data Theft to the List of Ransomware Cyber Risks

Ransomware gangs leaking data stolen from victims has appeared as a disturbing trend, with the primary reason ostensibly being to prompt their targets to pay sooner than later. Data theft has always been an often-unnoticed cyber risk in ransom scenarios, but now recent research is revealing that hackers are increasingly adopting this tactic in direct response to efforts to curb attacks. This strategy adds a new dimension to the already frightening predictions for malware surges in 2020 with the shift to the new normal and more employees working from home.

Here are the key items to know about the rise of hackers stealing data during ransomware attacks:

Hackers Leak Data to Incentivize Payment
Cybercrime has always relied on human error and emotion to execute on hacking campaigns and short-term goals, and this latest trend is a direct counterattack to the backlash against encryption attacks. Ransomware gangs frequently attempt to leverage the desperation of their victims by providing an air of courteousness, making payment seem like both a simple transaction and better than the alternative. These efforts to cultivate an agreeable reputation masks the lasting damage ransomware infections have, but momentum has progressively shifted against cooperation.

Between public opinion and regulatory action, there is a growing stigma against interacting with ransomware gangs in any form. Threatening to expose data is the next logical move for these cybercriminal groups as it reinforces the seriousness of their demands and the consequences of noncompliance.

Continued on page 2...

What our clients are saying:
Pee Jay's Fresh Fruit

"SWK did an amazing job during our office move! They were there for anything we needed."

Pamela Fisher
Pee Jay's Fresh Fruit

Two ways to WIN a gift card!

It only takes a minute and YOU could be our next winner!

Last Month's Contest Winner:

Amy Jo Morris
SobelCo

Please complete our brief survey in order to be placed in the running to win this month's gift card prize!

1. What do you like most about our services?

2. Tell us about a specific experience with us that you were happy with.

3. What are the biggest benefits you've received or experienced since hiring us?

4. What can we improve?

Email Jon Stiles (jonathan.stiles@swktech.com) with your responses
OR
Fill out our online form:
http://bit.ly/nwsnews-survey
before **Sept. 4th** to get your name in the hat.

You could win a $25 Gift Card!

Leveraging Virtualization Technology During the Pandemic

Several virtualization models have become increasingly popular during the coronavirus pandemic, including virtual desktop interface (VDI), virtual networks and more. Hosting your internal technology through virtual environments allows you to migrate away from static endpoints and workstations to a more flexible, scalable paradigm in which your users can move more freely. Leveraging virtualized servers, institutions like the city of Corona, CA have been able to completely shift to a remote workforce while saving IT costs.

Here are the key takeaways from the rise in virtualization technology use during the pandemic:

Growth of Virtualization Amidst COVID-19
Considerable research has been conducted into the growth of virtualized IT resource deployment from firms like Deloitte, Enterprise Strategy Group (ESG), and others, trying to chart the "virtualization of everything" spurred by COVID-19 and many other factors. The ESG study was carried out before the mass migration to work from home (WFH) environments, yet found many of the same drivers existed before and were only exacerbated by the pandemic. Multiple reports have shown that IT professionals and decision makers have a majority positive opinion of virtualized technology, and organizations are only moving increasingly to the cloud.

VDI, DaaS, Virtual Servers and More
The ESG report highlighted an interesting takeaway within the growing confidence in desktop virtualization - most of those surveyed were equally optimistic on all delivery models. This followed many trends found in a study by marketing firm Spiceworks, especially a lack of understanding of technology language. Decision makers are already planning to escalate their migration to virtualized solutions for data storage, software applications and network resources, but many seem to only have a high-level of the technical complexities between these tools.

Cybersecurity for Virtual Technologies
The journey to virtualization has already begun through increasingly digitized server resources, and the above research revealed this migration is only spreading out to other solutions. However, it is clear that knowledge around the various technology approaches and requirements is still growing, including for virtual IT cybersecurity. A few reports contained potentially contradicting results on the native security of virtualized systems, with respondents divided even amongst themselves about the benefits versus pitfalls.

Virtualization security reflects the demands of most digital infrastructure - every user becomes an endpoint, yet there is potentially more control at the administration level to quickly address threats. Protecting virtualized desktops, applications, and networks requires a vigilant team that knows how to balance resources efficiently, as well as identify and quickly handle intrusions.

Contact SWK Technologies to Learn More About Virtualization
The world is migrating increasingly to hosting network and IT resources in cloud environments, and digital computing infrastructures have been the driving force behind the new normal. Schedule a call with a support resource at SWK Technologies to learn how to leverage virtualization for remote work, and discover how we can protect your virtualized deployments to ensure disruptions do not interfere with your business.

Contact SWK Managed Cloud Services today to discover if virtualization is right for you.

Add Data Theft to the List of Ransomware Cyber Risks

Continued from page 1...

Legal, Healthcare and Finance Industries the Most Targeted
Businesses and institutions that are becoming the biggest target of this new tactic are those that the biggest incentive not to lose their data, such as legal firms, healthcare providers and financial services. In many of these sectors, personal data is a critical component of their operations and its exposure or loss could result in consequences for multiple stakeholders. Hackers are well aware of this and purposefully look for victims that too much to lose if they do not comply.

However, this group will very likely expand as data privacy laws taking root in states like California and New York compel businesses to both protect consumer information better as well report any potential theft. Once data is confirmed to have been stolen by an external party, companies could face greater losses than just from the ransomware itself.

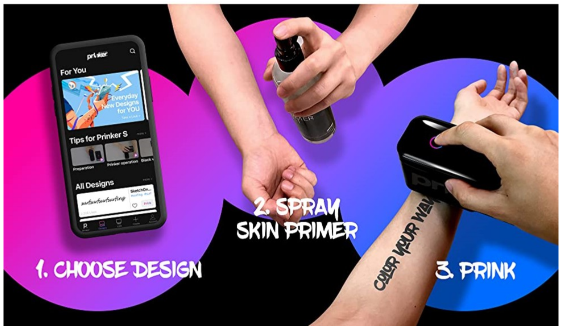
Data Leaks an Increasingly Popular Tactic
Examples of this emerging strategy have already made their way into the news as several unfortunate victims across the world have had their data breach exposed in various ways. One of the most popular now is the use of "data shaming," which typically sees the victim listed on a website or online forum explaining how they had been hacked. This listing remains until the ransomware gang finds a "buyer" for the data, most often the victim paying the ransom but can also include another party purchasing the information.

Ransomware Surging with Remote Work
So many individuals working from home in the midst of COVID-19 has contributed to a potential attack surface expansion for businesses nationwide, and hackers are trying their best to exploit it. Ransomware gangs have reemerged in the spotlight as one of the most prolific cybercriminal elements in the pandemic owing to so many easy victims for these attacks, which rely on volume. With how many remote workers rely on unsecure home devices and networks to access business data, all it takes is persistence for hackers to identify and breach someone to piggyback on for greater network access.

Stop Hackers from Using Your Own Data Against You
These are uncertain and chaotic times, and cybercriminals have historically become more active during these types of periods, trying to take advantage of emotionally vulnerable victims. Don't let disruptions distract from your network security - reach to SWK for help with deploying around the clock protection to help defend against data breaches.

Contact SWK Technologies today and learn how to spot and stop the preludes to a ransomware encryption attack.

Shiny gadget of the month: Prinker



There has been so much focus on work from home lately with everything going on (and rightfully so), but what about the day when we get back to normal? Truth be told this gadget seems like it will be just as much fun for using at home now, but it has some pretty cool applications for once we get back to normal and things like in person trade shows become a thing again. This gadget is called Prinker and it is a portable temporary tattoo printer.

The concept is really neat. You can print temporary tattoos anywhere. It has thousands of pre-done designs, but also gives you the ability to create custom ones. So whether you want to just play around with it at home and test out their designs, create one of your own for special occasions, or maybe you have thought about getting a tattoo, but wanted to see if you really liked it…this gadget can be the way to do it all. From a business standpoint bring one of these to the next trade show you have a booth at and do some personalized branding or just offer up some fun designs, it would be super unique and a fun way to engage with people.

The operation of Prinker is simple. Use the app to choose a design or draw your own, send it to the device using Bluetooth, prime your skin with their special primer spray, then slowly rub the device across the area to bring your tattoo to life. Everything is skin safe, waterproof and will last up to two days, but can be easily removed with soap and water at any time. Each cartridge holds enough ink to produce up to 1000 tattoos.

This is a really unique product that has so many fun and practical applications. It seems like such a fun thing for personal and professional use that luckily you don't have to choose between the two. The price tag is not super cheap, but for what trade show costs are $269 isn't that crazy, ink refills will run between $99 to $150 depending on color or not. You can find out more info for yourself on their website https://www.prinker.us/.

How to Protect Your Business Printers Against Hackers

Business printers are usually the last in a long line of physical and digital IT assets to protect against hackers, after your computers, servers and databases. Precisely because they're so overlooked, printer cybersecurity is often lacking and provides a gateway for bad actors looking to breach your network. Cybersecuring your whole network means securing your whole technology stack, and connected but unnoticed hardware equipment can create shadow IT holes in your security plan.

Here are the steps your business must take to ensure your printers are protected against hackers:

What Makes Business Printers So Vulnerable to Cyber Attack

Desktop computers, laptops and servers are much more noticeable in cybersecurity assessments because they are often the biggest vector for cyber attack. Printers are often at the bottom of the list for review since they are typically not prime targets, especially with how many older models companies employ. However, even some legacy business printers are increasingly being modified for wireless connections, and that means they are connected to your larger network. This is in and of itself, a significant attack surface expansion, but the purpose of printers also make them a critical overlooked vulnerability Businesses run important documents such as tax forms, employee information, medical records, and financial statements through print devices, and hackers would definitely love to get their hands on them.

Network printers store previous print jobs in their hard drive, sometimes including those that have been canceled. If anyone accesses the printer — even remotely — they may be able to see those documents by hacking into the printer using a specialized tool.

Files can also be intercepted during wireless transmission, as modern printers can now be connected to the web. Not only can hackers exploit printers' open network ports to view data, but they can also take over vulnerable printers and transmit their own data through the machine.

What You Can Do to Protect Your Business Printers from Hackers

Business printers should not be disregarded when planning a cybersecurity strategy. Keep your print devices secure by following these best practices:

- Monitor your network continuously and promptly install printer software updates and patches. Printer manufacturers often release software support or updates, so regularly check for those.
- Change the default password and administrator login credentials of printers with web management capabilities.
- Only allow company-owned devices to connect to your printers.
- Always connect to your printers using secure connections. Conversely, avoid accessing your printers through a public internet connection.
- Restrict printer access by using a firewall.
- If your wireless printer has the feature that requires users to enter a PIN before they can print documents, enable it to prevent unauthorized access.
- If you don't use your printer for fax and email, isolate your printer from your main company network and disable out-of-network printing.
- If you handle classified data, do not connect your printer to any network. Instead, connect it directly to your computer using data cables, or print from a thumb drive.
- Secure your printouts by enabling manual feed. This setting requires a user to manually input paper (or any material to be printed on), so there are reduced risks of the printed document getting stolen or being left in the printing area.

Contact SWK Technologies to Secure Your Business Printers

Engaging an experienced managed IT service provider is also a great way to ensure your business printers and other mission-critical assets are protected around the clock. SWK Technologies is an award-winning MSP that can protect your devices and IT infrastructure on-premise or in the cloud, and we monitor your devices regularly for cyber threats.

Contact SWK today to learn more about protecting your printers and other network assets.

Gift Card Trivia!

This month's question is:

What can you do to avoid SIGRed Found in Windows DNS Server? (Hint: The answer is in this newsletter.)

a. Install Anti-virus
b. Make sure your Windows systems are up to date and patched
c. Use a VPN
d. It can't be stopped

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **Sept. 4th,** in order to be placed in the running for this month's gift card prize!

We can help you with:

- Cybersecurity
- IaaS
- Complete network management and support
- Troubleshooting and problem solving on all PCs and Macs
- Cloud services and virtualization
- Hardware installation and support
- Virus / spyware removal and protection
- Security solutions
- Employee awareness training
- VPN (Virtual Private Networks)
- Remote access / Mobile computing
- Server installations and upgrades
- Spam filtering
- Hosted email
- Web content filtering
- System backups, on-site and off-site
- Help desk

Contact us

Give us a call for more information about our services and products.

SWK Technologies, Inc.

South Jersey
650 Grove Road, Suite 106
West Deptford, NJ 08066

North Jersey
120 Eagle Rock Ave., Suite 330
East Hanover, NJ 07936

Phone: 856.956.5800
Fax: 856.845.6466

Visit us on the web at
www.swknetworkservices.com

SWK
MANAGED CLOUD SERVICES

Remote Code Vulnerability SIGRed Found in Windows DNS Server

The remote code execution (RCE) vulnerability SIGRed was uncovered this past July, and affects all Windows DNS Server clients from Windows 2003 to Windows 10. Similar to past remote access exploits like 2019's BlueKeep, SIGRed was found to be a potentially wormable RCE security bug that could give a hacker full control of a machine. The true danger of remote code attacks, however, lies in how severe the cybersecurity gap is and if it allows the exploit to propagate across multiple computers.

Here are the key factors to know about SIGRed:

CVE-2020-1350 - Wormable Windows RCE Vulnerability
Officially labeled CVE-2020-1350 by Microsoft, the remote code execution exploit was first made public by security researchers at Check Point on July 14, 2020. Their studies identified a huge vulnerability within Windows DNS Servers, with DNS (Domain Name Systems) being the Internet directory that lists and generates your IP address from your computer hostname. This enables your browser to load Internet resources in the first place, though there are many other critical roles fulfilled by various DNS Clients.

SIGRed being wormable is what makes the severity so great, as a successful attack will grant the hacker full administrative rights for the servers, escalating the cyber threat beyond just a few machines. Additionally, the fact that it exists as far back as Windows 2003 indicates the vulnerability has existed in some form for 17 years.

CVSS 10 Score - What Does That Mean?
The Common Vulnerability Scoring System (CVSS) rarely grants a vulnerability the base score or 10.0, yet CVE-2020-1350 is considered so dangerous that Microsoft and even Homeland Security are sounding many alarms. In the latter case, the DHS's cybersecurity division gave federal agencies only 24 hours' notice to update and secure their Windows environments. In many ways, the longevity of SIGRed makes it even more of a risk than BlueKeep or DejaBlue, and its wormable nature puts it at the same or a worse level than the WannaCry or NotPetya ransomware.

Ensure that Your Windows Systems are Updated to Avoid SIGRed
Even Microsoft was releasing a fix for SIGRed during July 2020's Patch Tuesday, an additional RCE exploit was found affecting SharePoint, the .NET Framework, and Visual Studio. Windows systems are frequently targets of hackers for a few key reasons, the biggest being their worldwide ubiquity. The OS as well as MS Office applications are so widely used, that any exploit opens the door to data access for tens to hundreds of millions of victims.

This prevalence also means that any bad security practice that becomes common enough - like password reusage - still nets cybercriminals a large base to target and does half of the work for them. The recurring Windows bugs and lax personal cybersecurity means that Windows is constantly having to be patched, and users who fall behind on updates run the risk of being caught up by any new vulnerability.

Let SWK Technologies Manage Your Windows Environment
Microsoft updates, unfortunately, can present a risk themselves, but allowing a managed IT service provider like SWK Technologies to oversee your Windows upgrades will help you gain better control of your system. SWK's engineers are constantly monitoring both your network and the state of Windows' technology, so can help you navigate the complexity of each update.

Contact SWK Technologies to hear more about what we can do for your Windows systems.