IT Strategy Brief

ISSUE 8 | VOL 4 | August 2018

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:

Homeland Security Says ERP Vulnerable to Hacking

An alert released by US Computer Emergency Readiness Team (CERT) on behalf of the National Cybersecurity and Communications Integration Center (NCCIC), a division of the Department of Homeland Security, brought attention to a joint report by two cybersecurity firms revealing that hackers are showing renewed interest in Enterprise Resource Planning (ERP) solutions. According to the report, threat actors are targeting existing exploits in legacy ERP systems that allow for gaps that grant access deeper into the network the software if connected to.

ERP solutions are extensive and inherently complex software systems that are designed to facilitate application for critical operational functions. Additional integrations extend the functionality of ERP systems beyond core processes to allow for more specific roles to be managed through the software. Modern developments have expanded the reach of ERP solutions through cloud technology, yet the ubiquity of the Internet is one factor that contributes to broader attack surfaces in this type of software.

The report referenced research conducted on cybercriminal and nation-state actors exchanging information on the dark web and other online venues. Cyber-espionage groups have been exploiting loopholes in unsecured cloud services to breach enterprise network systems for some time already, and other groups are looking to combine gaps old and new as well. The NCCIC even referenced a previous alert from 2016 in the most recent warning as an indication that this is not an individual occurrence regarding enterprise software.

According to the previous bulletin, even though the existing vulnerability was patched long ago, it still provides an opening for attackers to exploit in outdated legacy ERP systems or those that have not been configured properly. This particular bug would allow someone to bypass any forms of authorization to obtain remote access to the system and any others it was connected to. It would also allow the attacker to completely control the ERP solution and all associated systems.

Continued on page 2...

What our clients are saying: Scirocco Financial Group

"One of the key issues for us is being able to consistently maintain our data, back up, have all information at hand at a moment's notice, and with that, SWK has performed a very, very big and helpful service to our organization in knowing the stability's there for us to have that information on an ongoing basis."

John Scirocco
Scirocco Financial Group

SCIROCCO GROUP INSURANCE

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Rolf Zezula
Technick Products

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 **September7th** to get your name in the hat.

You could win a $25 Gift Card!

Homeland Security Says ERP Vulnerable to Hacking

Continued from page 1…

This highlights the danger of these vulnerabilities existing within ERP software, as the primary function of these solutions are to oversee and manage core processes, as well as to integrate ancillary features into a centralized interface. ERP systems are by definition connected with the critical operations of your business, and the availability of Internet-facing functionality in modern ERP solutions can provide an external entry point to attackers if these gateways are not secured properly.

The alert is one of several efforts by the DHS to combat the frequency of network attacks and protect US commercial and public interests from these threats. Earlier in 2018, the Department also warned of suspected targeting of the US energy grid by Russian hackers and later they unveiled the creation of the National Risk Management Center, "a dedicated hub to helping private industry avoid and respond to cyberattacks from around the world," according to CNET. These moves indicate a renewed focus by the DHS on ensuring national cybersecurity, as well as the seriousness of the threat of network breaches to the private sector.

Read these 5 ways to maintain your ERP solution's data security from SWK's ERP practice, or sign up for a Network Vulnerability Test to get a better understanding of the state of your system's security.

Cybersecurity During Your Vacation

Cybersecurity might be one of the last things you want to worry about while enjoying your time off, but the increasing connectivity of the world means that protecting you networked devices is a constant fact of life. If you are one of the 95 percent of Americans that own a smartphone, the 53 percent that own a tablet, or your family is part of the third of US households that live with three or more mobile devices, then chances are that you will still be vulnerable during your vacation.

The primary factor in vacation cybersecurity is your mobile security as that is the vector with the most opportunities and the biggest attack surface to exploit while traveling. Many users do not often think twice about securing their smartphone (or tablet) and sacrifice protection for expediency, for both personal and business use.

There are a couple of key points to remember for staying safe and secure during your vacation:

- Be mindful of your network. Public Wi-Fi names that may seem innocuous can be spoofed by hackers, so that what you thought was your hotel's connection is actually a gateway into your data
- Be careful when using public machines too. The Department of Homeland Security released an advisory in 2014 announcing that several investigations had found keylogger malware installed in the business centers of several hotels
- Check your location data. Repeated instances of hidden iPhone tracking programs have made public just how easy it is to build a map of your travels using your phone's built-in GPS features. Even Android has gaps that could be exploited if someone is trying to locate you
- Keep your device up-to-date. Be extra mindful of what version of your OS is using, as occasionally the hardware does not keep up with the software and older systems will be missing security updates
- Watch what you post on social media. Hackers have been turning to social engineering to develop their attacks, and if they believe your credentials can grant access to critical data in some way, they will be following your movements.

Above all, remember that your Internet-connect machines can be a gateway to important data. You may not realize it, but every device you use brings at least some risk of an attacker trying to use it as an access point to personal or corporate information which they can exploit or sell.

Read through some of the ways employees do not realize they are leaving systems vulnerable to learn more about even the slightest mistakes can create network gaps.

Shiny gadget of the month: Sobro Coffee Table

Fall is approaching and that means that we will start spending more time indoors on our couch watching sports and TV in general. Have you ever been sitting there wanted a drink or a snack, but you are in the middle of a must watch moment of whatever you are viewing? The answer is yes, we all have been there at one time or another, but we may not have to be again…

The Sobro Coffee Table is the ultimate gadget for your living room. It is a coffee table, charging hub, storage space, sound system, light show, and is also happens to be a refrigerator. That is right, no more will you suffer having to get up from your couch, you can stash drinks or food right there in front of you. It has charging ports and your standard outlets build into it as well so everything is super accessible, so you don't have to try to find that plug behind your couch anymore. The table features Bluetooth connective speakers as well as LED lights you can use to add some ambience and fun. Everything is controlled right there on the table too, so no fumbling for an app on your phone to control things. Set the volume, turn on the lights, right there.

Sobro started out on Indiegogo where it crushed its funding goal back in 2017. It is out of the funding stage and has been shipping for some time. They have been featured all over in the press with publications like Forbes and Maxim leaving rave reviews. They have even begun developing a nightstand style version of this that will have even more features tailored to the specific needs you might have for a nightstand.

This stylish coffee table seems like it could really be the ultimate gadget for your home (or at least man cave). You can view their products on their website https://sobrodesign.com/ to see all the cool features.

Mobile Cybersecurity is Only Getting Worse

We have previously reported that businesses were found to be overlooking their mobile cybersecurity concerns by a Verizon research team. Almost a third of organizations surveyed were discovered to have sacrificed their security for expediency when using mobile devices, and nearly half of those had experienced system downtime or a serious data loss at some point. 89 percent of those examined employed nothing beyond the very basics of mobile cybersecurity measures, yet 93 percent claimed that these devices presented a growing threat to their business's network security.

Since the Verizon report was released, there have been similar warnings sounded by individuals and organizations coming from all sections of infosec, yet the outlook of mobile cybersecurity does not seem to have improved in any significant way. In fact, there are signs that it is likely getting worse for smartphone owners as hackers intensify their efforts to penetrate mobile networks and users continue to ignore best practices for protecting their devices.

Cybercriminals have found an avenue which allows them to easily bypass publisher safeguards for mobile applications and infect users with malware. This is made possible by "droppers," or applications which multiple-stage infection processes to sneak into a device's hard drive. Droppers hide within legitimate programs and further mask themselves by presenting the first stage as an easily removable threat.

IBM's X-Force research found that even after Google made efforts to eliminate this threat from its mobile Play Store, nearly two dozen of the same type of malware vectors remained. This particular malware, BankBot, tricks users into revealing their banking and credit card information. The seriousness of this specific program indicates an escalation building upon the ability of relatively more benign adware apps to infiltrate legitimate application stores.

Even while hackers improve their capacity to exploit gaps in mobile cybersecurity software, user practices exacerbate the problem. The Verizon report and other studies highlight that the human factor continues to create data protection openings, and even among federal employees and military personnel there is a gross lack of compliance with best practices among significant percentages. A survey of government employees found that 94 percent of Department of Defense personnel questioned had not had their personal devices approved by the agency.
Mobile cybersecurity is just as important, if not more so, as desktop security in safeguarding networked devices and critical data. Smartphone ownership is so widespread in the US that it is near-ubiquitous for every American household. Hackers realize this, and many are tailoring their efforts towards mobile platforms with nowhere near the amount of protection or oversight that desktop machines have warranted.

Check out our Phishing Defender solution to learn more about how you can train your personnel to recognize potential threats and help ensure best practices in your network operations.

Gift Card Trivia!

This month's question is:

What ERP systems are potentially exposed to increased risks from hackers?
(Hint: The answer is in this newsletter.)

a. New ERP systems that have not been configured
b. New ERP systems
c. Outdated legacy ERP systems or those that have not been configured properly
d. Outdated properly configured ERP systems

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **September 7th**, in order to be placed in the running for this month's gift card prize!

We can help you with:

- 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 TECHNOLOGIES

SEC Signals Tougher Stance on Financial Cybersecurity

In February of 2018, the Securities and Exchange Commission released an updated set of guidelines for public companies in disclosing cybersecurity risks and incidents. Though this guidance was presented as a collection of supportive best practices, the SEC has since followed through significantly on these protocols in the form of their ruling on the Yahoo breach revelation.

Altaba, as the remnant of Yahoo! Inc. is now called, was fined $35 million for failing to disclose that their infosec team had discovered that hackers had stolen their customers' login information. The penalty was levied against Altaba based on several factors, but primarily for failing to fully investigate the incident and properly disclose all of the details to investors.

"We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case," said Steven Peikin, Co-Director of the SEC Enforcement Division. Altaba, when it was still Yahoo, knew of the breach in 2014 but did not disclose it, and it was not discovered until 2016 while Verizon was finalizing its acquisition of Yahoo's assets.

The decision demonstrated the SEC's commitment to enforcing the new interpretation of cybersecurity obligations, but it also reflects a growing approach towards network security enforcement. Regulatory agencies have begun to expect an improvement of effort on the part of organizations which collect and manage the personal data of their personnel, customers, or membership. This is evident in the severity of some of the punishments, such as when a medical practice network in southern New Jersey was fined over $400,000 by the state for the actions of a contractor which exposed their patients' information.

Demonstrating best practices in protection non-public personal information (NPI), especially that of clients, is slowly becoming integral to compliance in multiple industries in several nations. Businesses will be increasingly called upon to display methodologies for preventing cybersecurity incidents as well responding to actual network breaches.

Contact us to find out how we can help you review your current network capabilities and ensure that you follow best practices in network security.