TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

March 2018

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Five Cyber Threats to Worry About in 2018

Hackers are constantly finding new targets and refining the tools they use to break through cyber defenses. The following are some significant threats to look out for this year.

More huge data breaches

The cyberattack on the Equifax credit reporting agency in 2017, which led to the theft of Social Security numbers, birth dates, and other data on almost half the U.S. population, was a stark reminder that hackers are thinking big

when it comes to targets. Other companies that hold lots of sensitive information will be in their sights in 2018. Marc Goodman, a security expert and the author of Future Crimes, thinks data brokers who hold information about things such as people's personal Web browsing habits will be especially popular targets. "These companies are unregulated, and when one leaks, all hell will break loose," he says.

Ransomware in the cloud

The past 12 months have seen a plague of ransomware attacks, with targets including Britain's National Health Service, San Francisco's light-rail network, and big companies such as FedEx. Ransomware is a relatively simple form of malware that breaches defenses and locks down computer files using strong encryption. Hackers then demand money in exchange for digital keys to unlock the data. Victims will often pay, especially if the material encrypted hasn't been backed up. That's made ransomware popular with criminal hackers, who often demand payment in hard-to-trace cryptocurrencies. Some particularly vicious strains, such as WannaCry, have compromised hundreds of thousands of computers. One big target in 2018 will be cloud computing businesses, which house mountains of data for companies. Some also run consumer services such as e-mail and photo libraries. The biggest cloud operators, like Google, Amazon, and IBM, have hired some of the brightest minds in digital security, so they won't be easy to crack. But smaller companies are likely to be more vulnerable, and even a modest breach could lead to a big payday for the hackers involved.

The weaponization of AI

This year will see the emergence of an AI-driven arms race. Security firms and researchers have been using machine-learning models, neural networks, and other AI technologies for a while to better anticipate attacks, and to spot ones already under way. It's highly likely that hackers are adopting the same technology to strike back. "AI unfortunately gives attackers the tools to get a much greater return on their investment," explains Steve Grobman, chief technology officer at McAfee.

An example is spear phishing, which uses carefully targeted digital messages to trick people into installing malware or sharing sensitive data. Machine-learning models can now match humans at the art of crafting convincing fake messages, and they can churn out far more of them without tiring. Hackers will take advantage of this to drive more phishing attacks. They're also likely to use AI to help design malware that's even better at fooling "sandboxes," or security programs that try to spot rogue code before it is deployed in companies' systems.

Mining cryptocurrencies

Hackers, including some allegedly from North Korea, have been targeting holders of Bitcoin and other digital currencies. But the theft of cryptocurrency isn't the biggest threat to worry about in 2018; instead, it's the theft of computer processing power. Mining cryptocurrencies requires vast amounts of computing capacity to solve complex mathematical problems, which is encouraging hackers to compromise millions of computers in order to use them for such work. Recent cases have ranged from the hacking of public Wi-Fi in a Starbucks in Argentina to a significant attack on computers at a Russian oil pipeline company. As currency mining grows, so will hackers' temptation to breach many more computer networks. If they target hospital chains, airports, and other sensitive locations, the potential for collateral damage is deeply worrying.

vmware PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

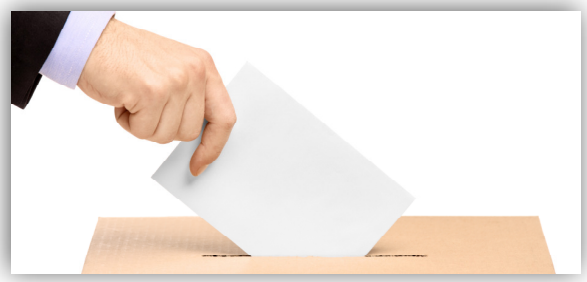
1-(800) 900-8324 (option 2)

Sales@TechHero.com

Hacking elections (again!)

Fake news isn't the only threat facing any country running an election. There's also the risk of cyberattacks on the voting process itself. It's now clear that Russian hackers targeted voting systems in numerous American states ahead of the 2016 presidential election. With midterm elections looming in the U.S. in November, officials have been working hard to plug vulnerabilities. But determined attackers still have plenty of potential targets, from electronic voter rolls to voting machines and the software that's used to collate and audit results.

As these and other risks grow in 2018, so will the penalties for companies that fail to address them effectively. On May 25, the General Data Protection Regulation will come into effect in Europe. The first big overhaul of the region's data protection rules in more than two decades, the GDPR will require companies to report data breaches to regulators—and inform customers their data has been stolen—within 72 hours of discovering a breach. Failure to comply could lead to fines of up to 20 million euros or 4 percent of a company's global revenues, whichever is greater.



2018's Cutting Edge Network Security Solution:

Cisco Umbrella

Cloud Delivered Enterprise Security

As the industry's first Secure Internet Gateway in the cloud, Cisco Umbrella provides the first line of defense against threats on the internet.

As a secure internet gateway, Cisco Umbrella helps you tackle the challenges of mobility, SaaS, and branch transformation by offering a single platform that secures access to and use of the cloud, SaaS applications, branch offices, and endpoints.

It's your first line of defense against threats -- anytime and anywhere your users access the internet, traffic goes through Umbrella first. By delivering security from the cloud, not only do you save money, but it also provides more effective security. Here's how:

1. DNS & IP layer enforcement

Umbrella uses DNS to stop threats over all ports and protocols — even direct-to-IP connections. Stop malware before it reaches your endpoints or network.

2. Intelligent proxy

Instead of proxying all web traffic, Umbrella routes requests to risky domains for deeper URL and file inspection.

3. Command & control callback blocking

Even if devices become infected in other ways, Umbrella prevents connections to attacker's servers. Stop data exfiltration and execution of ransomware encryption.

Call Tech Hero today to sign up for your free trial!

(800) 900-8324 x2

The recent revelation that Uber covered up a big cyberattack last year has sparked calls for breach disclosure rules to be toughened in America too. All this means that lawyers, as well as hackers, will have a very busy 2018.

Client Spotlight

Epilepsy Association of Central Florida

The Epilepsy Association of Central Florida is dedicated to improving the quality of life for children and adults with epilepsy and seizure disorders throughout Central Florida. Not only does EACF provide services for those with epilepsy and seizure disorders, but we also offer many programs and opportunities for your office/community/group to learn more about epilepsy.

To donate to this amazing organization please visit:
https://www.firstgiving.com/floridaepilepsy

Would you like your company highlighted here in our "Client Spotlight"? Then give us a call today at: 1-800-900-8324 x8840.

tech hero

FUTURE OF RANSOMWARE ATTACKS: MORE OF THE SAME, ONLY WORSE

As technology has evolved over the years, so have malicious actors. One of the worst types of malware, ransomware, has greatly affected numerous companies and individuals. Unfortunately, ransomware attacks are becoming more and more frequent. For example, the number of ransomware attacks in 2016 was 638 million. The attacks then rose an additional 250 percent in 2017.

An attack every 10 seconds

Ransomware is the most popular type of malware attack. Individuals are attacked every 10 seconds while businesses are attacked every 40 seconds, according to Kaspersky Security Bulletin. While you might think that only small, ill-equipped businesses are attacked and affected, this isn't true. A quarter of businesses that were attacked by ransomware have over 1,000

employees, and 71 percent of all companies targeted by these types of attacks were affected. The problem is that, with 4.3 times new ransomware variants just in the first quarter of 2017 compared to Q1 2016, it's difficult for security solutions to keep up.

Devastating effects of ransomware attacks

Ransomware can be devastating, corrupting all of the data on your network quickly, spreading from server to server and quickening as it spreads. Almost half of ransomware infects at least 20 employees by either encrypting files through shared network drives or finding multiple employees to fall victim to the initial attack. If we take a look at the polymorphic ransomware Virlock, each time you click on an affected file, the attack starts all over again, spreading even after you thought it was under control. On the other hand, ransomware attacks can also just make small, subtle changes over time that take weeks or even months to detect.

These two forms of ransomware both have a system that tries to avoid your security. If your data is corrupted rapidly, data protection solutions might not be able to handle the new rate of data churn. On the other hand, if the changes are subtle enough to not be caught for months, they could delete the uncorrupted copies of your data on your backup server before you realize anything is wrong.

RDP: An opening for ransomware

The majority of ransomware infections in 2017 were delivered via Remote Desktop Protocol (RDP), bypassing human error similar to the huge WannaCry attack. When attacking via RDP, attackers scan for open ports, similar to SMB break-ins. Then, once this is found, attackers brute force weak or default passwords, gaining entry. Many attacks in 2017 were performed this way, even though it is relatively simple for both businesses and individuals to secure against it. Although only about less than 5 percent of compromised companies pay the ransom, almost all businesses take at least

two days to get access to their files. This cost can be much more damaging to companies than the ransom itself. According to Imperva, every day of downtime can result in $5,000 to $20,000 in lost business and damages.

What's the solution?

One solution is eliminating credential reuse. While it's beneficial to not have too many top-level administrative credentials, it also isn't good if one administrator has too much access.

Additionally, if you backup your information to a site or the cloud, it should have separate credentials from your network so your backup will stay protected. Malware is able to "look at the backup server configuration, identify where it might be sending disaster recovery copies, then go infect those servers, effectively wiping out the entire organization by eliminating all of its data." Never browse the web as the domain admin.

While changing your credentials and separating files helps you keep a backup, it doesn't help protect against the attack in the first place. For this, the likely solution is machine learning so security solutions can keep evolving at a quicker speed than the malicious attacks are.

THE CHANNEL CO.
CRN
MSP 500
2017

Tech Hero

has made the Pioneer 250 list of CRN's 2017 Managed Service Provider 500 List!

The 2017 MSP 500 list recognizes companies in North America whose approach to delivering managed services is one innovative step ahead.

The MSP Pioneer 250 is a list of channel companies with business models weighted toward managed services and largely focused on SMB market.