inspired eLearning®
education for your enterprise

SECURITY AWARENESS

Wednesday, January 17, 2018

In This Issue

This Month's Tips:

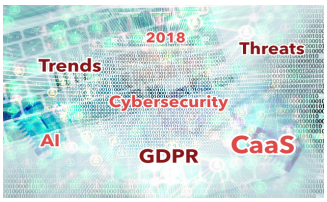
Create passwords that cannot be found in a dictionary or easily guessed.

Do not access workplace data on mobile devices unless authorized and necessary.

Let your friends know of any suspicious activity on their email accounts or contact lists.

Classify, label, and protect all documents and files according to organization policy to help safeguard them from malicious insiders.

Security Issues and Trends in 2018



It's a new year, and with that comes new threats and trends in the cybersecurity industry.

CaaS

CaaS, or Crime-as-a-Service, is when criminals develop advanced tools and other services that they later put up for rent or sale to other criminals, typically on the dark web. Think services such as on-demand denial-of-service attacks and bulletproof hosting to support malware attacks to name two. This is not a new concept, but as more criminal organizations partner together and collaborate on attacks, cyber incidents are becoming more sophisticated. Organizations must keep their security efforts up to speed to outpace cybercriminals.

Are you ready for GDPR?

On May 25th of this year, all organizations doing business with customers and organizations in the EU will need to comply with the new regulations outlined in the General Data Protection Regulation, better known as the GDPR. Organizations across the globe are scrambling to meet all the requirements by the May 25th deadline. With fines of up to 20 million euros or 4% of the total worldwide annual turnover from the preceding financial year, businesses will remain on their toes to see how vigorously these regulations will be enforced.

AI as an Enemy and a Friend

The cutting-edge capabilities of AI are now being exploited by cybercriminals as well as being used to protect from these attacks. What we might start to see in 2018 is AI versus AI, as both hackers and defenders use artificial computing power to launch and volley attacks. Organizations might use AI to fill the cracks in their defenses, while hackers use AI to find the one vulnerability they missed. At the end of the day, we just need to stay one step ahead.

Use parental controls to prevent your children from sharing personal information.

Cybersecurity Skills Shortage

With the increase of cybersecurity threats, more and more organizations are looking to hire specialized professionals to assist with protecting their businesses. But with increased demand and a small pool of experienced cybersecurity professionals, companies can expect to pay a lot for new talent or look to outsource.

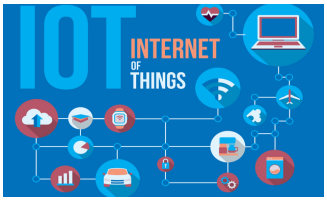
Thirty-Six Reasons to Monitor Your App Permissions

Android users hoping to take advantage of security apps offered on the Google Play store got a rude awakening when they found out their supposed "security" app was one of more than 36 that the store removed because the apps contained malware, adware, and spyware.

The security incident was discovered by Trend Micro (via ZDNet), who found that these apps advertised themselves as providing security and other useful capabilities, including cleaning up junk files. These malicious apps included those posing under names including Security Defender, Security Keeper, Smart Security, and Advanced Boost.

Once installed, the apps barraged the user with fake security alerts, while also collecting data, including the user's Android ID, the network operator, the brand and model of the device, and even its location. In order to avoid falling victim to intrusive malware, Trend Micro recommends users carefully examine app permissions – because an app that demands extensive permissions in order to perform basic tasks might be something sinister. "Be aware of the scope of app permissions. Apps sometimes require more than the basic default permissions. Make sure the installed apps only have access to features they need," the researchers said.

Are You Gifted?



While some of the most popular items being purchased for children this holiday season were *Fingerlings* and *L.O.L. Surprise! Dolls*. Internet of Things, or IoT devices, such as personal assistants for the home, tablets, and wearable fit devices, were the must have items amongst adults.

By now one could expect that those who have been gifted, or gifted themselves with an IoT device, have begun to incorporate it into their everyday life. Hopefully, after overcoming the excitement associated with having the latest gadget, some actions were taken to protect it from being hacked.

This is important because if protections are left unchecked, many IoT devices can cause some very serious problems down the road. With that being said, now is a great time to go over a few very simple things you can do to help protect your IoT gifts.

Step 1. Change the default password. Most people don't even know that many IoT devices have default passwords that should be changed to a strong password prior to use. A strong password should be as long as possible, unique yet easy to remember, never shared with anyone, and changed regularly.

Step 2. Check for software updates. To help prevent your IoT devices from being exploited, always check for the latest updates or patches from the manufacturer. This can help protect your device from security flaws and emerging threats.

Step 3. Disable remote or universal plug and play. Most internet-connected IoT devices come out of the box ready for action (and immediately connect to them). Read the information and instructions that came with the device to find out if it is plug and play and if so, turn it off. As a best practice only connect to secure networks.

Remember, IoT devices such as baby monitors, security cameras, smart thermostats, and televisions that connect to the Internet are all susceptible to hacking in the same way that mobile devices and laptops are, so they must be included as part of your overall security routine.

SPECIAL REPORT: Meltdown and Spectre in a Nutshell

What exactly are Meltdown and Spectre, and why all the hype about them? Are they two parts of the same threat? Are all computers and smart devices now rendered an open target for malicious hacks? Is there nothing we as consumers can do? Is the world of cyberspace coming to an end?

Not quite.

Meltdown is an exploit that affects an inherent vulnerability in the processor chip of a computer, smart device, or hypervisor (the hardware that supports virtual machines). The processor chip, or central processing unit (CPU), is at the heart of all computers and what makes them run. Meltdown essentially breaks down the walls, or containers, that keep data segregated by bypassing certain security measures that protect sensitive information.

The reason for all the sensationalism is that in the hands of an attacker, Meltdown will allow malicious programs to snoop around high-privileged parts of your computer's memory, giving the attacker access to your private files, passwords, or cryptographic keys. While this vulnerability has been known for at least a decade, it has just come to light by four independent research groups that Meltdown doesn't require physical access, rather nefarious hackers can breach any unpatched CPU from anywhere.

Spectre on the other hand, allows attackers to lift data from the memory of other applications you're running. Take this scenario for example, I have my online banking website open, and I get an email notification, so I open my email in another tab. The email says I need to confirm my upcoming appointment by clicking on a link. The link opens up another tab in my browser window. Now, while I am trying to figure out whether or not I made a doctor appointment on this fake but real-looking site, the attacker on the backend is pilfering my bank data that's two tabs over. Since Spectre is an attack with two known variants of execution, researchers expect to see more variants and similar exploits on the horizon.

Serious? Yes. Deadly? No.

Meltdown and Spectre exploits can cause serious widespread threat; however, no known exploits have cropped up in the wild, yet. In fact, before public announcements went out, many players in this field of technology were given a head start to "immunize" their software before their release dates. In addition, several key players in the processor space have issued software patches and firmware updates that will protect users from Meltdown.

Spectre, on the other hand, is a work in progress as it is a method of attack. Nonetheless, headway is being made on one of the variants of this exploit. Because Spectre patches require mitigation techniques that don't yet exist, software vendors need to do some work on their end, including updating their compiler infrastructure and recompiling their products for patches.

Experts point out that each of the patches don't actually remove the threat of attacks. They just reduce the likelihood an attacker will be successful. They maintain the only true fix is replacing a computer's CPU.

What can I as a consumer do?

Replacing a CPU is not like changing batteries. So, until CPU architectural designs have been rethought out and are in the works, we as consumers need to be vigilant.

- Be on the lookout for phishing scams, fake updates, and too good to be true deals on quick fixes for Meltdown and/or Spectre.
- Always type in the URL or go to the official website of your product for updates and patches.
- Don't wait! Update as soon as your product patches are made available: anti-virus/anti-malware software, firmware, OS, and browsers.

To prevent attackers from gleaning information across browser tabs in a Spectre attack, update to the latest Chrome browser and enable the Strict Site Isolation (SSI) feature so each tab/page will load separately from differing servers.

To do this, type *chrome://flags/#enable-site-per-process* into your Chrome browser window and click the toggle button to enable Strict Site Isolation.

Bottom-line

Just as buffer-overflow vulnerabilities and Heartbleed led to years of vulnerable programs, Meltdown and Spectre will have a similar impact on the security landscape. With knowledge comes power, THINK before you CLICK!

Inspired eLearning | 613 N.W. Loop 410 | Suite 530 | San Antonio, TX 78216
