The Beacon

Florida Fusion Center #15-143 Cyber and Critical Infrastructure Report October 2015 Issue #8

Contents

Summary

Training Your "Cyber Gut" — Most cyber incidents are caused by human error...which means they are mostly preventable. This article discusses ways to develop an instinct to recognize when things aren't right in your cyber world.

The Culture of Cyber Security — Organizations large and small all must prioritize cybersecurity to their employees. We provide some helpful tips to train employees on handling sensitive information.

Before You Enter the Cloud — More and more individuals are using "the cloud" to store their data. But what is it? And is it secure? We give you an overview about what you need to know before entering the cloud.

Internet of Things: Rise of the Machines — As more devices connect to the Internet, how concerned should we be about security?

Cyber Security: The Next Generation — As the song goes, "I believe the children are our future, teach them well and let them lead the way." It is important that we train the next generation of Internet users so they understand the risks associated with unlimited access to information.

About *The Beacon*

The Secure Florida Beacon is published by Secure Florida to highlight cyber and critical infrastructure security information and awareness.

Secure Florida is an Internet safety and awareness effort of the Florida Department of Law Enforcement's Florida Infrastructure Protection Center (FIPC). The FIPC was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a team of cyber intelligence and critical infrastructure protection analysts. FIPC analysts work to protect Florida's infrastructure through FDLE's Internet safety and awareness effort (Secure Florida), and the website SecureFlorida.org.

If you see a topic where you would like more detailed reporting, or have seen something you think we need to know about, Let Us Know.

Contact SecureFlorida.org at:
(850) 410-7645
Admin@SecureFlorida.org

Editor's Corner

National Cyber Security Awareness Month

Since 2004, each October has been designated as National Cyber Security Awareness Month by the Department of Homeland Security. In order to commemorate the month, every week has a different theme related to the topic of cyber security. In keeping with this, we decided to organize this issue of the Ledger around each week's theme.

There are five focus areas during this year's National Cyber Security Awareness Month:

Week 1: General Cyber Security Awareness: 5 Years of Stop. Think. Connect.™

In 'Training Your "Cyber Gut,"' we talk about general tips for keeping Americans safe online.

Week 2: Creating a Culture of Cyber Security at Work

'The Culture of Cyber Security' discusses why it is important that, as employees, we take care to protect our organization's networks in the same way we do our home networks.

Week 3: Connected Communities: Staying Protected While Always Connected

We should protect our smartphones and mobile devices just as we protect the computers that sit on desks. Our article 'Before You Enter the Cloud' examines why we need to protect our data wherever we access it from, even when on the go.

Week 4: Your Evolving Digital Life

Our article 'Internet of things: Rise of the Machines' focuses on this week's theme of looking at where technology is today, and where cybersecurity professionals see technology moving in the future.

Week 5: Building the Next Generation of Cyber Professionals

Our article "Cyber Security: The Next Generation" discusses the importance of teaching all young people to have a good cyber security posture, even if they aren't studying for a career in IT.

To find out more about National Cyber Security Awareness Month, please visit:
http://www.dhs.gov/national-cyber-security-awareness-month

Cyber Highlights

Cyber Highlights represent issues cyber analysts have seen active in Florida. The following articles are intended to serve as overviews of issues we feel the citizens of Florida would benefit from knowing.

Training Your "Cyber Gut"

This month marks the 13th anniversary of FDLE's Secure Florida initiative, and the 5th anniversary of the STOP.THINK.CONNECT.™ campaign, which started as a global cyber security awareness effort sponsored by a handful of federal agencies.

While the security incidents we see may have changed, they remain an ever present danger to Internet users. Crafty criminals constantly find new ways to circumvent security systems and processes. A well informed and security conscious public is crucial to protecting cyber resources; you can become your best defense against loss.

Systems may fail, but you can, in essence, train your "cyber gut" to sense when things aren't right online.

Here are three simple lifestyle adjustments you can make to increase your cyber vigilance:

- **Work to improve your password creation and use skills.** Just like working to develop the skills that help you improve a sport, board game, or crossword puzzle, you can work on using better passwords through practice. To develop a better security stance, increase your password's length each time you create a new one. Passwords are the one element of cyber security over which you actually have a great deal of control. We discuss more about what makes a good password in this issue's article about the cloud. Remember, the better you make your password, the harder a hacker has to work to crack it.

- **Always be skeptical when it comes to downloading files from websites.** Do your homework. Some places are quite safe to download from, and others are set up to fool you into downloading malicious files. This is one time that it's okay to always have that "gut feeling" that something is not right. Do some research-- Google or Bing can help you see if others have had good experiences (or bad) with a program you find online.

- Almost everyone uses social networks these days. And why not? They are a fun way to keep up with friends and family. However, anytime you put something online make sure you understand who all can see it. Sites like Facebook, Twitter or Instagram have default privacy settings that may share info in ways that you are not comfortable with. **Research privacy settings, routinely; they often change without fanfare.** It's okay to be a skeptic and raise an eyebrow when it comes to privacy settings.

There is more you can do, but you can start with these simple steps to help develop a better "cyber gut" when it comes to determining when things just aren't right.

The Culture of Cyber Security

The trend of cyber intrusions affecting some of our nation's most prominent firms and businesses shows no sign of slowing down. However, corporations now recognize the need for innovative approaches to cyber security as incidents reveal the impact even a single breach can have on their organization. IT security traditionally focuses on hardening infrastructure from attacks, but ultimately it is the human component that is vital to security. Employees at all levels within an organization must understand the critical elements of cybersecurity and what they can do to safeguard both themselves and their organization's data.

One of the best methods to prevent these cyber breaches from crippling an organization is to foster a culture of security, which means making security a priority in all business activities. Below are questions developed by Microsoft that employees should ask themselves when handling sensitive information:

- Is this something that can be thrown away or does it contain sensitive information that should be shredded?
- How well do I know this person on the phone and should this conversation be happening?
- Do I trust the sender of this email? Is this link or attachment in the email safe to click?
- Is the stranger approaching me with questions that seem too personal? Am I offering up detailed information that could be damaging if it fell into the wrong hands?
- Is this information something that should be shared on social media for everyone to view?[1]

Employees need to understand not only the characteristics of external cyber threats, but also the policies and practices they are expected to follow in their work environment.

Below are four important elements of a strong cyber defense strategy, according to the Workgroup for Electronic Data Interchange (WEDI) Perspectives on Cyber Security in Healthcare June 2015 Report:

1. Have basic controls in place to mitigate threats. These include up-to-date operating systems, web filtering, and antivirus software. Put in place firewall technologies to stop known attacks. Set up automated alerts that quickly notify the appropriate parties and help activate response measures.

2. Train employees at all levels, to cultivate awareness of ongoing cybersecurity issues.

3. Develop a response system that can identify a breach at its source as well as the scale of the compromise.

4. Respond to any attacks that have breached the network. Establish a coordinated response plan for breaches.[2] Resources are available through federal partners including the Multi-State Information Sharing and Analysis Center at soc@cisecurity.org.

A company's leadership can only form a functioning cybersecurity culture by including the entire workforce, from the average employee to the top executive, in training and response measures.

[1] Baker, Ann and Kaplinska, Kasia. "Creating a culture of security." 13 February 2015. <https://www.microsoft.com/enterprise/it-leaders/cybersecurity-privacy/articles/creating-a-culture-of-security-in-your-enterprise.aspx#fbid=oGSc1GOhYQJ>.

[2] "Perspectives on Cybersecurity in Healthcare." 2015. <http://www.wedi.org/docs/test/cyber-security-primer.pdf?sfvrsn=0>.

Before You Enter The Cloud

"Mobile computing." It's the buzz phrase of the decade. We want to work on the same files from our offices, our hotel rooms, and best of all our homes and our recliners. Maybe even on the beach. Yes, you can carry your files around on a flash drive, but what if it ends up lost or stolen? What if the files contain sensitive material?

Many people turn to the cloud. And, while it solves the problem of access, it may be introducing a whole other issue of security. Of course, security has always been an issue, even at the local level. Disgruntled employees, unpatched systems, weak passwords…these pose a threat in the real world as well as in the cloud. Still, there's that feeling that if the security is out of your control then there is a bigger risk.

Here are several important steps to protecting your information.

Do your homework

The first step is research, research, research. Although we frequently speak of "the cloud," there are in reality several variants of the cloud. Your choice will probably depend on what type of service you need: storage, backups, document collaboration, infrastructure, or technical support, just to name a few.

Also, look for compatibility. Make sure that the cloud you select works with your software and files. Finally, you need to decide between the public and private clouds. In general, the public cloud is perceived as the less secure but the more financially feasible option. Also worth considering are hybrid solutions that may better suit your needs. *For Dummies* provides a comprehensive look at each of the three options: http://www.dummies.com/how-to/content/comparing-public-private-and-hybrid-cloud-computin.html.

Read the contract/user agreement/terms of service

Once you have identified the features you need, spend some time carefully reading the contract. Yes, it's boring and confusing; but it's essential. Make sure your data belongs to you exclusively. While this likely seems obvious, in 2012 Google Drive came under fire for claiming the rights to anything a user uploaded, in perpetuity. You also want to find out where your data, and any backups, will be stored. If they are kept outside the U.S., does that present any security or legal concerns?

Ensure you receive high-level security

Insist on a detailed description of the security layers that will be protecting your information. Make sure they are at least as robust as the security you have now.

What is the Cloud?

Some of us may dabble in it; some may depend on it. Some may even use it unknowingly. But what exactly is it that we are trusting with our data?

The cloud is merely a series of large computers (servers), stored in warehouses around the world. They provide software, services, and data storage; both for organizations and individuals. Anyone who has used Google Drive, iCloud, or Dropbox has benefited from the cloud, although they may not realize it.

Interesting Fact:

The entire cloud can store roughly 1 Exabyte of data: that's 67 million 16GB-flash drives![1]

Some advantages:

- Files are accessible 24/7 from any device connected to the Internet.
- You have all the storage you need, and it's easily expandable.
- Your data is available even in times of disaster.

Some disadvantages:

- Without an Internet connection you have no access to your files.
- You must trust a third party to protect your (sometimes critical) information.
- Cloud servers are a prime target for hackers due to the wealth of information they contain.

Use strict password rules

You've heard these recommendations from the FIPC before, and probably from every other security-focused organization. But 90 percent of people fail to follow them. And a machine running an efficient password-cracking program can crack any eight-character password in about five hours. (http://www.infosecurity-magazine.com/news/90-of-passwords-can-be-cracked-in-seconds/)

Sometimes the strength of your password is limited by the program, account, or site you are trying to access. But wherever possible, passwords should:

- Be at least 15 characters long
- Have combinations of upper and lower case letters, numbers, and punctuation
- Not contain words found in any dictionary
- Be different for all important accounts and sites
- Not be written down where someone else can find them

If you are wondering how to create a strong yet memorable password, try Googling "how to create a strong password that's easy to remember." You'll find several suggestions; just pick the one that seems to work best for you. Remember that length wins over complexity.

Use encryption – for storage and transmission

Both encryption and passwords protect your data, but encryption is much stronger. Using a password is like putting your documents into a safe and then locking it. If a safecracker were to successfully open the safe, the documents would be easily accessible.

Encryption, on the other hand, is like first shredding your documents and then locking them in the safe. Even if the safecracker opens the safe (that is, cracks your password), your documents are still undecipherable. It takes an encryption key to successfully restore them.

Some cloud services provide their own encryption, However, if you are interested in getting your own encryption software, the link below is a good place to start:

http://encryption-software-review.toptenreviews.com/

[1] **Al-Greene, Bob. "How Big Is the Cloud?" 4 October 2012. <http://mashable.com/2012/10/04/how-big-is-the-cloud/#ZnGZT2PeTPkR>.**

Internet of Things: Rise of the Machines

Should we be worried about the Internet of Things (IoT)?

In the beginning, a virus typically spread via sharing floppy disks...but then came the Internet. Viruses, worms and other malware were free to wreak havoc all along the information highway. As anti-virus companies worked to stop the spread of malware throughout the Internet, they realized that the bad guys seemed to always have the upper hand. As soon as vendors released a patch, bad guys would develop a new variant of the malware to target computers.

Today we are still one step behind, but the kinds of devices that we are connecting to the Internet are constantly expanding. An unsecure IoT becomes a great target for ransomware, botnets, and hackers. As McAfee Labs noted in its five-year threat review released in September (http://www.mcafee.com/us/about/news/2015/q3/20150901-01.aspx), cybercrime has become an industry with all the operational trappings of any legitimate sector. The IoT is fairly young, and data breaches and device hacks are just beginning to make headlines. From cars and medical devices to industrial control systems, anything that is "connected" is now a potential target. A big part of the problem with securing the IoT is that many firms making these newly connected gadgets have little experience with the arcane world of computer security, if the need for security is even mentioned.

As the IoT matures, the warning lights are flashing for security professionals. In 2014, researchers discovered a botnet of digital video recorders (DVRs) owned by other people. The sabotaged machines spent their time crunching through the complicated calculations needed to mine bitcoins for the botnet's controllers. The controllers of the botnet were able to successfully control the DVRs without alerting the real owners to any of the mining activity.

There will always be bad players in the Internet world, and many of them are going to target the IoT. We need to make sure our security practices keep pace with what could be a whole new world of nastiness online.

Cyber Security: The Next Generation

Cyber attacks have evolved over the course of the last few decades. It used to be that viruses and malware smacked the user in the face when they infected a computer; nowadays, malicious actors largely operate in the background, with users unaware of their existence until a great deal of damage has been done. The "next generation" of cyber attacks will continue to evolve, as malicious actors find new ways to exploit vulnerabilities in networks.

To combat this, development of new technologies is important. However, as the tactics and technologies employed by malicious actors grow and change, there must be a greater emphasis placed on building and encouraging the next generation of cyber security professionals.

The Next Generation of Cyber Professionals

The U.S. Department of Labor estimates that by 2020, the country will have 1.4 million information technology specialist jobs.[1] Because this sector of the economy will only continue to increase in size and importance, it is vital that all levels of the educational system provide a focus on cyber and cyber security. In the not-so-distant future, virtually all industries will require a cyber element, and fostering interest in the field will aid in building a culture of cyber professionalism in the coming decades.

There are numerous training programs for young folks interested in the field of cyber security. For example, Honolulu Community College hosts a weeklong summer camp to educate high school students on cybersecurity principles and guide the professional development for those interested in pursuing higher education in cyber-related fields of study.[2] This past summer, the National Security Agency coordinated a number of summer camps hosted at colleges across the country to teach students about cyber security.[3]

Other organizations exist in order to balance gender representation in the cyber field. Girls Who Code (girlswhocode.com) is a nationwide nonprofit which teaches computer science to grade school girls and exposes them to leaders in the tech industry to encourage young women into tech fields and decrease the gender gap.

Cyber Awareness is Everyone's Responsibility

Not every one of today's students will embark on a career in cyber. However, as our world becomes increasingly connected and reliant on the Internet, it is incumbent upon all of us to have a certain baseline of knowledge when it comes to cyber security.

Schools should provide a focus on educating the younger generations about cyber security and the threats that exist in cyberspace. Formal curriculum should exist for all students on core cyber security concepts such as knowing one's digital footprint and best practices for protecting one's sensitive information from cybercriminals. In today's world, it is no longer appropriate for anyone to remain ignorant about cyber security fundamentals, because the Internet affects everyone's lives every day.

[1] Labor, U.S. Department of. "Bureau of Labor Statistics." 2014. <http://www.bls.gov/ooh/computer-and-information-technology/computer-and-information-research-scientists.htm>.

[2] Ching, Kapi'olani. "Booting up the next generation of cyber security professionals." University of Hawai'i News 20 July 2015. <https://www.hawaii.edu/news/2015/07/20/booting-up-the-next-generation-of-cyber-security-professionals/>.

[3] "NSA's Cyber Camps Make Summer School Fun." 11 May 2015. <https://www.nsa.gov/public_info/press_room/2015/gencyber_summer_camps.shtml>.

Dispatch Highlights

This section highlights articles from past FIPC Dispatches that our analysts think are noteworthy based on trends we're seeing in Florida. The FIPC Dispatch is a list of open-source articles that is sent out twice weekly. If you are interested in receiving *The FIPC Dispatch* LET US KNOW.

This content is intended as an informative compilation of current/open-source cyber news for the law enforcement, cyber intelligence, and information security communities.

26 Android Phone Models Shipped with Pre-Installed Malware

http://thehackernews.com/2015/09/android-smartphone-malware.html

- Many smartphone models from Chinese companies came equipped with non-removable spyware.
- The spyware is capable of many things, including listening in to phone conversations and messages.
- Security researchers suspect third parties are behind the malware, not the manufacturers.

Analyst Note: It doesn't matter who installed the malware, it's important that it was discovered. This is a good warning to readers to be wary of software AND hardware you purchase, because either may result in you sharing information you do not want to share.

How to cure Windows 10's worst headaches

www.pcworld.com/article/2975289/windows/how-to-cure-windows-10s-worst-headaches.html

- Any current user of a Windows operating system was offered a free upgrade to Windows 10 this summer.
- While many found Windows 10 to be a great improvement over Windows 8, users discovered a variety of privacy and security changes.

Analyst Note: This article walks you through how to change some of the default security settings which may compromise your privacy. When you get a new computer, device, or operating system, always verify the settings to ensure you are comfortable with the information your device may be sharing.

Here's How to Use Facebook's Mystifying Privacy Settings

http://www.wired.com/2015/08/how-to-use-facebook-privacy-settings-step-by-step/

- While the purpose of social media is to share, default privacy settings may result in you sharing more information than you would prefer.
- Facebook is notorious for sharing user information with advertisers, and its data policy reflects this.

Analyst Note: We often talk about your online footprint. Social media is the most common way that one's footprint grows larger, because they don't take care to keep their privacy settings in check. Always keep a close eye on your social media settings to avoid accidental over-sharing.

CONTENTS

Bad Guys Are Already Compromising Chip and PIN Cards

http://www.infosecurity-magazine.com/news/bad-guys-are-already-compromising/

- The chip-and-PIN system for credit and debit cards has long been used in Europe, but has slowly come into use in the U.S.
- While this technology is supposed to be a more secure method and less prone to scams, criminals have already begun to develop ways to get around the security features.

Analyst Note: With every new, more secure technology comes smart criminals who can figure out the weaknesses. Even though chip and PIN cards ARE more secure, it is still important to monitor your accounts to ensure you do not become a victim of identity theft.

Hackers Now Going After Ashley Madison Targets

http://techcrunch.com/2015/08/24/hackers-now-going-after-ashley-madison-targets/

- In July 2015, a group called "Impact Team" stole a large amount of data from infidelity website Ashley Madison.
- Following the initial threats, the group released information on approximately 31 million accountholders, including credit card data, as well as internal corporate data.
- As a result of this breach, criminals have begun to exploit Ashley Madison users whose information was released, attempting to blackmail them or utilize the data for identity theft.

Analyst Note: ANYONE can be a victim of a data breach. And regardless if it is a website for those seeking extramarital affairs or the point-of-sale systems for large retail corporations, victims may become a target for criminals seeking to use your information for personal gain. Those who initially cause the breach of information are not always the only criminals who will take advantage of that data.

The Dispatch is a bi-weekly compilation of open-source cyber and information security news. If you are interested in receiving The Dispatch, sign up here: http://eepurl.com/bdU8GD.