Colleagues,

2016 was an interesting year for cybersecurity professionals, with two key cybersecurity reports being released in December. From the DNC, to Dyn and Yahoo, hacks, breaches, and malware were discussed in the news throughout the year. The year ended with President Obama implementing economic sanctions against Russia and the expulsion of 35 Russian officials, and the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a Joint Analysis Report (JAR). The JAR provides "technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities." Previous JARs have not attributed malicious cyber activity to specific countries. This JAR is the first to do so. I recommend you read the 13-page report (https://www.us-cert.gov/sites/default/files/publications/JAR_16-2029A_GRIZZLY%20STEPPE-2016-1229.pdf).

The second report released in December was the President’s Commission on Enhancing National Cybersecurity (https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf). The Commission identified six imperatives for enhancing cybersecurity, with 16 recommendations and 53 actions to be taken by the next administration. The report is comprehensive, clearly articulating the depth and breadth of the cybersecurity challenges we face and recommendations to address those challenges. A common theme throughout the report is an emphasis, and recommendation, for everyone to use the Cybersecurity Framework for cyber risk management. The six imperatives the Commission identified are:

- **Imperative 1**: Protect, Defend, and Secure Today’s Information Infrastructure and Digital Networks
- **Imperative 2**: Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy
- **Imperative 3**: Prepare Consumers to Thrive in a Digital Age

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.
Police ask Alexa: Who dunnit?

By Elizabeth Weise, USA Today
December 29, 2016

In what may be a first, police in Arkansas asked Amazon for recordings potentially made by an Echo device in connection with a murder investigation.

Police in Bentonville, Ark., asked Amazon for audio and other records from an Echo digital assistant in the home of James Andrew Bates after Victor Collins was found dead in Bates' hot tub last year, The Information reported Tuesday.

Bates was charged with killing Collins on Nov. 22, 2015, according to court documents.

The two had been drinking and watching football with two other friends in Bates' home. One of the friends left, but Collins and another stayed after Bates told them they could sleep on the couch and an extra bed, the affidavit for a search warrant said. Bates went to sleep, and sometime in the night, Collins died in the home's hot tub, according to the affidavit.

The cause of death was strangulation with drowning as a secondary cause, according to police. Bates was arrested and charged with the murder. He is out on bail.

Amazon declined to provide the data.

"There's enough concern about the potential privacy implications of an always-on recording device in the home...”

Amazon refused both times. In a statement to USA TODAY, Amazon said it will not release customer information without a valid and binding legal demand properly served on it. Amazon objects to overly broad or inappropriate demands as a matter of course, the company said.

Amazon did give prosecutors information about Bates' account and purchase history. According to court documents, police took the Echo and extracted information from it, though what they would have been able to get isn't clear.

Bates' lawyer, Kimberly Weber, said that although her client is innocent and will be exonerated, she is concerned about the precedent of a search warrant including information from his Echo.

“I have a problem that a Christmas gift that is supposed to better your life can be used against you. It's almost like a police state,” she said.

How much does Alexa remember?

The Amazon Echo is an always-on digital assistant that can answer questions, order items and stream music, among other tasks. It supports Amazon's voice-recognition program Alexa, which operates in the cloud.

The devices are very popular. According to Amazon, the Echo and the smaller Echo Dot sold in record numbers this holiday season, nine times over the sales in 2015. Though Amazon doesn't give exact information on how many Echos it has sold, it did say "millions of new customers will be introduced to Alexa" as a result of sales this holiday.

It's important to note that "always listening" doesn't mean "always recording." The Echo is actually always listening only for its “wake word,” which by default is the name of its voice recognition program Alexa.

The Echo keeps less than 60 seconds of recorded sound in its storage buffer. As new sound is recorded, the old is erased. So there's no audio record made of what went on in a room where an Echo sits.

Read the rest here:
Membership Update

Congratulations to our new President, Colleen Murphy, and all the other new and re-elected board members. We are holding steady on our membership—~468 members as of the end of 2016. Overall, we are maintaining our membership with renewals and new memberships—both general and students/Freemiums. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

ISSA International will be briefing the Board at some point early this year with recommended changes to the Freemium program. It looks like there will continue to be some form of free student memberships available but the exact form of the new program remains to be determined. As soon as we hear what the new program will entail we will get that information out to the membership. In the interim, the Freemium program remains in place for Colorado Springs and Central Maryland chapters. So, if you’re thinking of recommending it to someone, please do so as soon as possible.

We still need more mentors! We have more people who want mentoring than we have mentors to support the program. Please contact Melissa Absher or me if you can support this worthwhile program for the chapter. It’s a good block to have on your resume when you submit your application for Senior Member, Fellow, or Distinguished Fellow.

Finally, I would like to welcome our new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information. Thanks for joining the Chapter and don’t forget to look for opportunities to lend your expertise to improve the Chapter. We’re always open to new ideas and suggestions.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

(Continued from page 1)

- **Imperative 4:** Build Cybersecurity Workforce Capabilities
- **Imperative 5:** Better Equip Government to Function Effectively and Securely in the Digital Age
- **Imperative 6:** Ensure an Open, Fair, Competitive, and Secure Global Digital Economy

If you don’t have time to read the report, you can jump to Appendix 1, on page 53, and just scan the table of Imperatives/Recommendations/Action Items. I challenge each of you to read – or at least scan – the report.

Last year was a very successful year for our Chapter. We hosted two conferences, a cyber technology day, a CISSP seminar, two Security+ seminars, several mini-seminars, and monthly lunch/dinner meetings. As your new President, I intend to continue those events in 2017, adding others where possible. As the President’s Commission on Enhancing National Cybersecurity final report shows, there’s a lot of work to be done, in many areas, to improve cybersecurity. Our Chapter will continue to do its part in providing a forum for cybersecurity professionals to network, further their education, and enhance their career growth.

I look forward to supporting all of you and leading our Chapter through the year.

Colleen
The Colorado Springs ISSA Chapter has over 400 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Shawn P. Murray at 5871charlois@gmail.com or at 719-362-0666 to coordinate the process. Shawn is the chair of the chapter awards committee and will help you through the steps. Below are some additional details on the ISSA Fellow Program. Qualification information is also presented below:

No more than 1% of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of 2% of the membership.

Nominations and applications are accepted on an annual cycle. The current cycle opened December 2, 2016 and applications will be accepted until July 10, 2017, at 5:00pm Eastern Time. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2016 ISSA International Conference. Submissions received after August 1, 2016 will be considered in the following cycle.

Familiarize yourself with the Fellow Program, and the submission guidelines (http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/Fellow_Program/Fellow_Policies_Revised_June.pdf). If you have questions, contact Shawn or The ISSA Fellow Manager (fellow@issa.org) or call 866 349 5818 (US toll free) extension 4082.

**To Become a Senior Member**

Any member can achieve Senior Member status. This is the first step in the Fellow Program. What are the criteria?

- 5 years of ISSA membership and 10 years relevant professional experience
- All Senior Member applications require an endorsement from their home chapter to qualify.

For your convenience, please feel free to use this Senior Member Application Check-list to confirm eligibility and completion of application

To access the Senior Member application go to: https://www.issa.org/?Senior_member_App
For the Senior Member endorsement form go to: https://www.issa.org/?Senior_Mem_Endorse

**To Become a Fellow or Distinguished Fellow**

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow. Please contact Shawn and become familiar with the Fellow Program Guidelines and use the current forms to ensure you comply with all requirements.

- 8 years of association membership, 3 years of volunteer leadership in the association and 5 years of significant performance in the profession such as substantial job responsibilities in leading a team or project, performing research with some measure of success or faculty
ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

Blue Ribbon Trophies & Awards

245 E Taylor St (behind Johnny’s Navajo Hogan on North Nevada)

Colorado Springs

(719) 260-9911

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.
Training and Education Update

Hello, my name is Luke Ingerman and I am your new VP of Training and Education! I have been participating in the ISSA Training Committee for the last several years and have trained Information Security and Risk Management portion of the CISSP and facilitated a CAP study group. I look forward to expanding my role with the ISSA Colorado Springs Chapter and working with the group to expand our training and education offerings over the next two years. As always, this program succeeds and grows based on participation and feedback from our members so please feel free to stop me at a meeting, or drop the team an e-mail at Training@issa-cos.org.

Sincerely,
Luke Ingerman, C|CISO, CISSP, CAP
ISSA-CoS, VP of Training and Education

Mini-Seminars

Mini-seminars are designed to provide members an opportunity to learn something new, and earn a few CPE/CEUs, at no cost. Mini-seminars provide continuing education, professional collaboration, and career broadening for members. They’re also a great opportunity for members to share their knowledge and experience with other members of the Chapter, and gain experience as a speaker, by volunteering to present a topic. Mini-seminars are generally held on a Saturday, from 9am – noon.

Mini-seminar topics and presenters from 2016 include:

- Payment Card Industry Data Security Standard (PCI DSS) - Presented by Art Cooper
- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) - Presented by Mark Spencer
- Security in Solution Architecture - Presented by William (Bill) Blake
- Social Engineering - Presented by Debi Caldwell
- Impact of Internet of Things on Privacy & our lives - Presented by Srikant Mantravadi
- Managing IT Security Projects - Presented by Russ Weeks
- Risk Management Framework for Leadership - Presented by Kurt Danis
- Risk Management Framework Working Group and Q&A - Presented by Don Brackett
- How do we keep the lights on when everyone has access to the switch? (i.e. SCADA) - Presented by Wally Magda
- Windows 10: It Begins with Securing the Endpoint - Presented by Al Green
- Cybersecurity Certifications - Presented by Kurt Danis
- Proactive Response Cybersecurity - Presented by Root9B, Mr Keith Smith
- Intro to Cryptography - Presented by Mark Heinrich

Are you missing out on a great opportunity for FREE continuing education credits? Are you missing out on an opportunity to share your knowledge/experience with your fellow Chapter members? Come to our mini-seminars and collaborate with your colleagues! Watch for info on topics and dates for our mini-seminars in future newsletters.

Security+ Seminars

Security+ Exam Prep Review Seminars are generally offered two times a year. All material has been reviewed and updated per the 2015 CompTIA SY0-401 criteria. The Security+ Seminar provides a comprehensive review of the CompTIA Security+ material to help students prepare for the Security+ exam. The 12-hour seminar is taught by certified Security+ or CISSP Chapter members, on two consecutive Saturdays, 9:00am to 4:00pm. Watch for dates for our Security+ seminars and registration details in future newsletters.

CISSP Seminar

The CISSP Exam Prep Review Seminar is offered once each year. The CISSP Seminar provides a comprehensive review of the (ISC)2 CISSP material to help students prepare for the CISSP exam. All material has been reviewed and updated per the 2015 (ISC)2 Common Body of Knowledge (CBK) criteria. The 40-hour seminar is taught by certified CISSP Chapter members, on five alternating Saturdays, 8:15am - 4:45pm. Watch for CISSP Seminar dates and registration details in future newsletters.
Continuing Education (CEU/CPE) Ideas

Do you know there are numerous free or low cost CEU and CPE options available? Check out the ISSA-COS web page (http://www.issa-cos.org), Training Classes, “On-Line Training” link for suggested sites.

Volunteer Opportunities

Looking for a volunteer opportunity? Looking for a way to share your knowledge/expertise? Looking for a way to earn CompTIA CEUs or (ISC)2 CPEs? We’re always looking for members to teach one or more of the Security+ or CISSP domains. We provide the slides, but you can modify them as you see fit as long as your changes remain consistent with the official CompTIA or (ISC)2 criteria. If you would like to volunteer to teach one of the Security+ or CISSP domains, or if you have questions, please contact our Training Committee leads at: Training@issa-cos.org. If there’s a topic you’d like us to cover during a mini-seminar, please let us know and we’ll see if someone in the Chapter is willing to develop a presentation for it.

If you have ideas/suggestions/requests for training initiatives, please email our Training Committee leads at: Training@issa-cos.org.

4th Annual ISSA COS Cyber Focus Day

March 30, 2017
University of Colorado Colorado Springs (UCCS)

University Center - Berger Hall
Colorado Springs, CO

https://www.fbcinc.com/event.aspx/Q6UJ9A015FRD

7th Annual Cyber Security Training & Technology Forum (CSTTF)

August 30th & 31st, 2017
Double Tree Hilton Hotel • Colorado Springs, CO

https://www.fbcinc.com/e/csttf/
Air Force Academy class develops software to solve cyber issues

By Wayne Heilman, Colorado Springs Gazette, December 8, 2016

A class of Air Force Academy cadets has come up with a novel solution to keep track of and solve cyber issues for Air Force Space Command - mobile and online applications that use a chat room, user ratings and other features more commonly found on social media than in a military network.

The 15-member Innovative Design class, working with six local industry experts, was asked in August by a Space Command unit to develop a better way for commanders to determine the risk a cyber problem poses to the unit and who is trying to solve it. They unveiled their prototype Wednesday that includes a chat room, an incident response reporting system, a glossary of acronyms and terms and a map that shows the location and severity of the problem as well as the ability to click on any part of the map to get a more detailed view.

"This class was more than what I expected it to be. They provided us with a different way of thinking than I have seen before at the Academy," senior cadet Everett Montano said. "There was no instructor teaching us; the class did the work. We weren't given a goal of what the product should look like. No idea was off limits."

The application, called the CyberWorx Responsive Dashboard, is designed to be used by Air Force personnel ranging from the lowest-ranking airman to wing commanders at any location as a way to crowdsource solutions to cyber problems ranging from a slow internet connection, inability to log into a key system or a network vulnerability. The dashboard allows users to rate posts as a way to automatically integrate the best solutions to common problems into a self-help resource that subsequent users can use to solve the problem themselves.

The class used a concept called "design thinking" in which those involved determine how to solve a problem and how they want that solution to work rather than asking an engineer to solve a technical problem, getting a solution months later and being told how to interact with it. The class and its assignment were developed by the academy's CyberWorx program, which teams military and industry personnel to solve cyber security problems and will present the cadet-developed application next month to the 24th Air Force, Space Command's computer warfare arm.

A key part of the demonstration the class gave Wednesday included a skit during which a pilot couldn't get medical clearance to fly because a router problem in the base's medical clinic prevented personnel there from logging into the clinic's scheduling system, nearly forcing cancellation of a training mission.

"They didn't just see this as a technology problems, but went to the root of the problem, which is how people to interact with each other. The problem has to be handled faster, and how you do that is by getting more eyes on the problem," said Col. Jeffrey Collins, director of CyberWorx. "Crowdsourcing is a spot-on solution to the problem of mission assurance. I don't care who fixes the problem because if the maintenance group can't pump gas (because of a computer issue), we can't fly. I love what you (members of the class) did because you showed a real-world problem."

Read the rest here: http://gazette.com/air-force-academy-class-develops-software-to-solve-cyber-issues/article/1591907
On Thursday, changes to a little-discussed rule will go into effect and will expand the United States government’s surveillance capabilities after several attempts to halt the rule change failed.

The changes in question to Rule 41 of the Federal Rules of Criminal Procedure would grant judges the ability to issue warrants that would allow for remote access, search, seizure, or copying of data when the location of said data has “been concealed through technological means” or when the information is located on protected devices and have been “damaged without authorization and are located in five or more districts.”

The rule would grant this power to any judge in any district where activities related to the crime in question may have taken place.

On its face, the rule change may seem innocuous, but privacy advocates have been arguing for Congress to disavow the amended clause since it was first presented in April of this year.

The primary concern is the potentially overextending power the rule would grant judges issuing search warrants. The rule could be used to issue remote access warrants that would allow the FBI the ability to hack devices that are physically located out of their jurisdiction or overseas.

On a more fundamental level, privacy organizations like the Electronic Frontier Foundation (EFF) and Access Now believe the rule may present a threat to just about anyone using basic privacy tools like Virtual Private Networks (VPNs) or the Tor browser that can conceal a user’s location and online activities.

In a blog post, EFF’s activism director Rainey Reitman warned the rule could be applied to even more basic levels than that, stating to could extend to “people who deny access to location data for smartphone apps because they don’t feel like sharing their location with ad networks” or to those who change their country setting in an online service like Twitter.

The rule could also have implications for users who are compromised by malicious software and made the victim of someone else’s activity.

For example, the botnet that took down major web services earlier this year via distributed denial of service attacks utilized hacked Internet of Things devices to deploy its bombardment. The changes to Rule 41 could give federal agents the ability to remotely access any computers or devices—and all the personal information stored within—used in that attack as part of an investigation, even if the only crime of the device owner was falling victim to a hack.

The ill-defined parameters of the tweaked Rule 41 leaves a considerable amount of room for overreach, leaving much to the jurisdiction of a judge who may or may not know exactly how much leeway they are granting to government agencies.

The FBI squarely blamed Russian intelligence services on Thursday for meddling in the 2016 U.S. presidential election, releasing the most definitive report yet on the issue, including samples of malicious computer code said to have been used in a broad hacking campaign.

Starting in mid-2015, Russia's foreign intelligence agency, the FSB, emailed a malicious link to more than 1,000 recipients, including U.S. government targets, the Federal Bureau of Investigation said in a 13-page report co-authored with the Department of Homeland Security.

While the Department of Homeland Security and Office of the Director of National Intelligence had said Russia was behind the hacking in October, the report is the first detailed technical analysis provided by the government and the first official FBI statement.

The findings come the same day that President Barack Obama announced a series of retaliatory measures, including the expulsion of 35 Russian intelligence operatives and the sanctioning of the GRU and FSB.

While the Department of Homeland Security and Office of the Director of National Intelligence had said Russia was behind the hacking in October, the report is the first detailed technical analysis provided by the government and the first official FBI statement.

The findings come the same day that President Barack Obama announced a series of retaliatory measures, including the expulsion of 35 Russian intelligence operatives and the sanctioning of the GRU and FSB.

The FBI said hackers gained access to and stole sensitive information, including internal emails "likely leading to the exfiltration of information from multiple senior party members" and public leaks of that information.

The report did not name hacked organizations or address previous conclusions reached by the Central Intelligence Agency and FBI, according to U.S. officials, that Russia sought to intervene in the election to help Trump, a Republican, defeat Clinton.

Trump has praised Russian President Vladimir Putin, tapped people seen as friendly to Moscow for administration posts and rejected assessments by intelligence agencies on the hacking.

Read the rest here:
http://www.reuters.com/article/usa-russia-cyber-fbi-idUSL1N1E01D1
The House Permanent Select Committee on Intelligence today released a declassified version of its investigative report on Edward Snowden, the former National Security Agency contractor who fled to China and then Russia after stealing an estimated 1.5 million classified documents. The report, including redactions for classified information, was the result of a two-year inquiry into Snowden’s background, likely motivations, and methods of theft, as well as the damage done to U.S. national security as a result of his actions. The report was completed in September 2016 and submitted to the Intelligence Community for a declassification review.

Intelligence Committee Chairman Devin Nunes said, “I’m gratified that, with the completion of the declassification review, the American people can now get a fuller account of Edward Snowden’s crimes and the reckless disregard he has shown for U.S. national security, including the safety of American servicemen and women. It will take a long time to mitigate the damage he caused, and I look forward to the day when he returns to the United States to face justice.”

Intelligence Committee Ranking Member Adam Schiff said, “Snowden and his defenders claim that he is a whistleblower, but he isn’t, as the Committee’s review shows. Most of the material he stole had nothing to do with Americans’ privacy, and its compromise has been of great value to America's adversaries and those who mean to do America harm. Whistleblowers are important to proper oversight and we will protect them from retaliation, and those who engage in civil disobedience are willing to stay and face the consequences.”

NSA and Cybersecurity Subcommittee Chairman Lynn Westmoreland said, “The American people have every right to know the extent of the damage Edward Snowden did to our national security, and I applaud the declassification of the House Intelligence Committee’s report. Not only did Snowden endanger American service members, threaten critical relationships across the globe, and reduce our allies’ ability to counter terror attacks, but repairing the damage he did cost a tremendous amount of taxpayer dollars and more importantly, used up valuable time and resources that should be spent keeping our country safe. This extensive report shows Snowden is no hero, and that he should be brought to justice for his reckless actions.”

Read the report here:

Read Intelligence Committee highlights of the report here:
Before You Pay that Ransomware Demand...

By Brian Krebs, Krebs on Security, December 22, 2016

A decade ago, if a desktop computer got infected with malware the chief symptom probably was an intrusive browser toolbar of some kind. Five years ago you were more likely to get whacked by a banking trojan that stole all your passwords and credit card numbers. These days if your mobile or desktop computer is infected what gets installed is likely to be “ransomware” — malicious software that locks your most prized documents, songs and pictures with strong encryption and then requires you to pay for a key to unlock the files.

Here’s some basic advice about where to go, what to do — and what not to do — when you or someone you know gets hit with ransomware.

First off — breathe deep and try not to panic. And don’t pay the ransom.

True, this may be easier said than done: In many cases the ransom note that hijacks the victim’s screen is accompanied by a digital clock ominously ticking down the minutes and seconds from 72 hours. When the timer expires, the ransom demand usually goes up or even doubles. Continue to ignore the demands and your files will be gone, kaput, nil, nyet, zilch, done forever, warns the extortion message.

See, the key objective of ransomware is a psychological one — to instill fear, uncertainty and dread in the victim — and to sow the conclusion in the victim’s mind that any solution for restoring full access to all his files involves paying up. Indeed, paying the ransom is often the easiest, fastest and most complete way of reversing a security mistake, such as failing to patch, opening a random emailed document e.g., or clicking a link. But they still want you to know that your choice is a binary one: Pay up, or kiss your sweet files goodbye forever.

This scenario reminds me of the classic short play/silent movie about the villainous landlord and the poor young lady who can’t pay the rent. I imagine the modern version of this play might go something like...

Villain: You MUST pay the ransom!
Victim: I CAN’T pay the ransom!
Villain: You MUST pay the ransom!
Victim: I CAN’T pay the ransom!
Hero: I’ll pay the ransom!
Victim: Oh! My hero!
Villain: Curses! Foiled again!

Okay, nobody’s going to pay the ransomware demand for you (that’s only in Hollywood!). But just like the hero in the silent movie, there are quite a few people out there who are in fact working hard to help victims avoid paying the ransom (AND get their files back to boot).

Assuming you don’t have a recent backup you can restore, fear not: With at least some strains of ransomware, the good guys have already worked out a way to break or sidestep the encryption, and they’ve posted the keys needed to unlock these malware variants free of charge online.

But is the strain that hit your device one that experts already know how to crack?

Where to go?

The first place victims should look to find out is nomoreransom.org, a site backed by security firms and cybersecurity organizations in 22 countries. Since its launch on July 25, 2016, nomoreransom.org estimates that it has been able to save 6,000 victims of ransomware more than $2 million USD to date. Last week the group announced the site is now available in Dutch, French, Italian, Portuguese and Russian.

Read the rest here:
https://krebsonsecurity.com/2016/12/before-you-pay-that-ransomware-demand/
Mitigating internal risk: Three steps to educate employees


IT security is usually focused on how to prevent outsiders with malicious intent from causing harm to your IT systems and data. While this is a valid concern, people within organizations who simply do not understand the consequences of their everyday habits and behavior on company computers pose an equivalent if not greater risk.

Every person within a company that has access to information is a gateway for data exfiltration. This is why education for ALL employees that encourages following best practices for IT security safety is extremely important to implement within organizations. So where should you start? Take 3 easy steps.

1. Awareness about the ways hackers get into your organization

The average computer user has most likely heard all the keywords – virus, firewalls, malware, phishing, ransomware, insider threats – but what it all means has to be explained at the basic level and the consequences need to be emphasized. Of course, the biggest emphasis should be on how hackers can use them to get access to company data. From experience, it's always best to use real-life examples.

Case in point: Recently, I worked with a university whose administration staff received an email to update their account information and passwords. It was a phishing scam that provided the hackers with multiple administrators' passwords. When I further investigated the issue alongside the IT security team, I realized people didn’t understand that it’s not as easy as just changing your password again and that it’s not someone manually digging through their information.

The department put forward an initiative to explain how phishing scams work and that the consequences are someone has all the data you had access to – including people’s personal data. In particular, most likely due to the high success rate of the hackers the first time, this university’s administration team was targeted multiple times afterwards. The hackers, however, failed to extract any additional information due to the administration’s teams new set of knowledge who reported each phishing e-mail afterwards and started a university wide alert every time they received a suspicious e-mail.

2. Constant reminders to change people’s bad habits

When employees first start it’s important to give them a list of the top 10 rules they should follow regarding IT practices. If you know the rules that are violated the most, it’s suggested that those should make the top of your list. If you don’t then a good way to find out is to use monitoring techniques that will help you to collect this data. There’s a high chance you’ll be surprised by the type of rules people violate. Some examples of no-no’s can include attaching company files to personal e-mails, putting data on non-encrypted USBs, uploading files to cloud drives etc. Yearly training and reminding sessions should also be implemented as a part of company strategy.

One of the most effective tactics is to inform users that they are violating policies while they’re attempting to take the action. This approach is extremely important for organizations who do not block particular actions because it can interfere with everyday tasks. For example, if someone in the customer chat department was to send a file via instant messenger, your IT team could set up a technology interface or leverage solutions that automatically alert the violating staff member – with a message saying that the action is not recommended.

Based on my own research with practitioners, in 72% of cases this was found to be enough to deter the user from completing the action. Furthermore, my research showed that 57% of actions that were going to be taken, could have led to data exfiltration.

3. Lead by example

Management can scare employees into following company policies but sometimes they don’t scare themselves enough. I’ve come across hundreds of companies where statistics show that management violates more IT policies than the average employee.

Read the rest here: https://www.helpnetsecurity.com/2016/12/20/mitigating-internal-risk/
Cybersecurity Ghosts of Past, Present, and Future

By Erin O’Malley, Security Week, December 15, 2016

Although an analysis of the latest government statistics confirms continued growth in the information security workforce, the supply of security expertise isn’t meeting the demand.

Thirty-some-odd years ago, my older brother wrote a “book” entitled The Christmas That Was Coal. It begins with a tale of a boy who’d been very naughty (not unlike Cousin Constantine), followed by a few more miscellaneous short stories, including (a personal favorite) “Christmas on the Moon.” Every year, my parents set that fabric-covered, satin-ribbon-wrapped book on their coffee table. And every year, I read it. Just as I do Charles Dickens’ A Christmas Carol.

Much as I love my brother’s oeuvre, it’s the Dickens that tops my list of annual, near-ritualistic indulgences. Never has it ceased to kindle nostalgia for the past, encourage awareness of the present, and sound a cautionary note for the future. In other words, it’s my time to reflect, take stock, and look forward.

And if you’ll indulge me, I’d like to steal you away, as did Ebenezer’s ghosts, for a wee journey down cybersecurity lane. See how far we’ve come, and where we’ve yet to go.

The Cybersecurity Ghost of Christmas Past

Last Christmas, I gave you my heart . . . Wait, no. I didn’t. Sorry about that. And besides, we need to go a bit further back than that anyway. Back to the early 80s when films like Red Dawn, The Day After, and WarGames had me shaking in my red Swoosh Nikes. Back to when President Reagan announced the Strategic Defense Initiative. Back to when the network started to take hold and when people started to care about network security.

In the 80s, ARPANET led to the Internet, which, in late 1988, was temporarily crippled by the first significant denial of service (DoS) attack—the Morris worm. Created and launched by a lone grad student, the worm was a wake-up call for a complacent online community, forcing it to take security more seriously and even giving rise to the Internet security profession.

With the 90s and naughts came more malware (worms, viruses, Trojans, bots), but also more security technologies such as antivirus programs, SSL encryption, stateful and stateless firewalls, DLP (birthed in 2007, resurrected in 2016), and all variety of intrusion detection and prevention systems. Businesses began to depend more and more on the Internet and, as would follow, its security. And average Joes began to realize they couldn’t blindly trust, say, emails from unknown sources or that everything that goes out over the Internet is safe (e.g., email is forever, and it’s not private).

The Cybersecurity Ghost of Christmas Present

Today, one thing is certain. Perimeter security is as dead as a door-nail. Or is it?

Some say yes, and that the mobilization of the workforce has made it irrelevant, that firewalls can no longer keep the bad guys out. This contingent believes it’s necessary to work under the assumption that most—if not all—networks have been breached, and that time and resources should be dedicated to limiting the blast radius of attacks.

Others disagree, saying perimeter security has just been improperly handled and must be deployed as part of a defense-in-depth strategy. So don’t go doing away with traditional perimeter defenses, but augment them, you know, maybe with better visibility inside the network in order to uncover and block malicious lateral movement.

Read the rest here:

GET A JOB!

Colorado Springs ISSA chapter member Melody Wilson maintains a “Jobs” page at Cyberjoblist.com. There is no charge. The jobs are set to remain listed for 30 days. Job listing originators re-post them again for another 30 days. It is designed for Colorado Springs, but once in awhile a job is listed outside the area.

You can also sign-up on the Cyberjoblist.com site for Job Alerts to be notified when a new job listing is posted!
Intelligence or Not Intelligence? That is the Question.

Contextual Intelligence Derived from Deep & Dark Web Data Can Deliver Truly Invaluable Insights

By Josh Lefkowitz, Security Week, December 5, 2016

As the saying goes, it’s not about what you do IF you’re attacked, it’s what to do WHEN you’re attacked - or worse, when you’re breached. And with more interconnectivity across business, government, users and suppliers, cyber attackers have a vast, data-rich environment to target.

Prior to co-founding Flashpoint, I spent the majority of my career focused on applying intelligence to support counterterrorism. I have seen firsthand what works in both private and public sectors, and how confusion around the topic of cyber threat intelligence (CTI) can create unnecessary hurdles for organizations trying to move quickly to thwart would-be or current attackers.

Since we founded the company almost seven years ago, the definition and value of CTI has become even more convoluted and opaque, which challenges me personally as an intelligence professional at my core. While markets must be dynamic with different offerings for organizations to determine their best protection and mitigation strategies, the increasing number of newcomers offering what they consider to be a variation of CTI has only increased this confusion. Because the definition of CTI has become so vague, attempts to differentiate can misshape market conversations and make it even more difficult for buyers of CTI to determine exactly what intelligence — if any — they are actually getting.

As we are often asked to define what is or is not intelligence, I want to dig into the different types of “intelligence” available on the market and review how that intelligence may or may not help organizations with their CTI strategies.

Open Web Intelligence

Most organizations track online mentions of their brand and stakeholders via search engines, social media, paste sites, and other open web sources. However, by the time such information reaches the open web, it is likely outdated, has already been exploited by threat actors operating within the Deep & Dark Web, and is ultimately insufficient for helping organizations proactively address critical threats and mitigate risk.

Despite widespread agreement regarding the relatively low value of open web data, the term “open web intelligence” appears to be gaining traction throughout the CTI industry. The problem is, open web “intelligence” is not intelligence. It is data.

Data is an integral component of intelligence, but failing to distinguish between the two can be problematic. Finished intelligence requires both data and context, and context requires a comprehensive understanding of the specific problem the data will address. It is nearly impossible to form relevant context without first considering how the data relates to the entire threat landscape. In the case of cyber intelligence, the threat landscape’s primary facets can be largely observed within the Deep & Dark Web, not the open web. Observing only the open web is not enough to develop context and thus cannot enable organizations to apply and operationalize the data to address their challenges effectively.

Above all else, the danger with open web “intelligence” practices is that they can mislead organizations into believing they have full visibility into the cyber threat landscape when the opposite is true. While open web data can certainly be useful, the most successful intelligence programs recognize that open web occurrences do not tell the whole story and simply indicate what may be happening within the Deep & Dark Web. Even further, the widespread content and behavioral moderation occurring throughout many open web sites is making it even more difficult to gain material visibility from such sources.

Full Coverage

Unfortunately, the unicorn of “full coverage” of the Deep & Dark Web continues to plague the industry. The Deep & Dark Web is immeasurably vast, contains dangerous regions, and is extremely difficult to access. The requisite highly-advanced cultural and language skills alone serve as substantial barriers for most organizations. Establishing trust with threat actors is absolutely critical and can only be achieved with the proper language and cultural skills. Without fluency in Arabic, Russian, Mandarin, and many other languages, it is impossible to accurately monitor threat actor activities and glean actionable insights — much less attain “full coverage” of the Deep & Dark Web. And while language skills are integral, fluency alone is insufficient; individuals seeking access to the Deep & Dark Web must have an intimate familiarity with certain communities’ social and cultural norms, vernacular, and idioms.

Second, entering the Deep & Dark Web also requires highly-advanced operations security and technical skills. Not only is gaining access to these online communities extremely difficult, it is risky. Without proper skills and precautions, an individual’s identity (and affiliated organization) can easily become exposed, rendering them vulnerable to vicious exploitation, retaliation, and substantial reputational damage.

Read the rest here:
http://www.securityweek.com/intelligence-or-not-intelligence-question
The Botnet That Broke the Internet Isn’t Going Away

By Lily Hay Newman, Wired, December 9, 2016

When the botnet named Mirai first appeared in September, it announced its existence with dramatic flair. After flooding a prominent security journalist’s website with traffic from zombie Internet of Things devices, it managed to make much of the internet unavailable for millions of people by overwhelming Dyn, a company that provides a significant portion of the US internet’s backbone. Since then, the number attacks have only increased. What’s increasingly clear is that Mirai is a powerfully disruptive force. What’s increasingly not? How to stop it.

Mirai is a type of malware that automatically finds Internet of Things devices to infect and conscripts them into a botnet—a group of computing devices that can be centrally controlled. From there this IoT army can be used to mount distributed denial of service (DDoS) attacks in which a firehose of junk traffic floods a target’s servers with malicious traffic. In just the past few weeks, Mirai disrupted internet service for more than 900,000 Deutsche Telekom customers in Germany, and infected almost 2,400 TalkTalk routers in the UK. This week, researchers published evidence that 80 models of Sony cameras are vulnerable to Mirai takeovers.

These attacks have been enabled both by the massive army of modems and webcams under Mirai’s control, and the fact that a hacker known as “Anna-senpai” elected to open-source its code in September. While there’s nothing particularly novel about Mirai’s software, it has proven itself to be remarkably flexible and adaptable. As a result, hackers can develop different strains of Mirai that can take over new vulnerable IoT devices and increase the population (and compute power) Mirai botnets can draw on.

“It’s accelerating because there’s a wide-open, unprotected landscape that people can go to,” says Chris Carlson, vice president of product management at Qualys. “It’s a gold rush to capture these devices for botnets.”

Internet of Bots

The rise of Internet of Things malware is reminiscent of the viruses, worms, and intense email spam that plagued early internet users. Most PCs weren’t adequately secured, and companies racing to join the dot-com bubble didn’t necessarily understand the importance of internet security. The same is true now, but with webcams and routers instead of desktops.

What’s distinctly different in this tech generation, though, is how users interact with infected devices. An infected PC often malfunctions, slows down, or notifies users (either through operating system security alerts or through the malware itself in the case of something like ransomware). All of this encourages people to act. It’s standard practice to install some sort of security software on enterprise PCs, and anti-virus measures are popular at home as well.

IoT devices like routers, though, are workhorses that are meant to function indefinitely, with minimal direct user interaction. One reason Mirai is so difficult to contain is that it lurks on devices, and generally doesn’t noticeably affect their performance. There’s no reason the average user would ever think that their webcam—or more likely, a small business’s—is potentially part of an active botnet. And even if it were, there’s not much they could do about it, having no direct way to interface with the infected product.

“The early 2000s web security called and they want their lack of security back,” says Rick Holland, vice president of strategy at the cybersecurity defense firm Digital Shadows. “It’s not like this population of total vulnerable devices is going to be going down. It’s going to be increasing.”

Hard to Kill

Mirai isn’t the only IoT botnet out there. The broader insecurity issues of IoT devices are not easy to address, and leave billions of units vulnerable to all sorts of malware.

But Mirai is the main go-to for now because it’s easily accessible and adjustable, with different strains for different campaigns. Holland says that Digital Shadows researchers have observed a growing community of Mirai users asking for help (even bad actors need tech support sometimes!) and offering each other tips and advice.

There are some precautions consumers can take to improve their personal IoT security. By assessing the IoT devices they have in their homes and eliminating superfluous “smart” products that directly access the internet for no reason, people can reduce their exposure to attack. Additionally, for devices that offer accessible interfaces, you can change default passwords and download firmware updates to get greater protection.

Mirai will ultimately be a “transient threat” in the broader landscape of IoT security, as a report published this week by the Institute of Critical Infrastructure Technology notes. Hackers get bored with shiny new toys just like anyone, and eventually the IoT industry will erode Mirai’s vulnerable device population.

Read the rest here:
https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/
Here are some best practices for preventing DDoS attacks

By Bob Violino, ZD Net, December 8, 2016

Distributed denial-of-service (DDoS) made lots of headlines in late October when a massive DDoS attack on Domain Name System (DNS) service provider Dyn temporarily disrupted some of the most popular sites on the internet.

As with any other major cyber security breach, the attack likely has many boards of directors and CEOs wondering whether their organization might be next, and what can be done to defend against such incidents.

DDoS attacks are clearly on the rise. A report by content delivery network provider Akamai earlier this year said such incidents are increasing in number, severity and duration. It noted a 125 percent increase in DDoS attacks year over year and a 35 percent jump in the average attack duration.

Not surprisingly, many people want to know more about these types of attacks. When the Software Engineering Institute (SEI) at Carnegie Mellon University recently posted a blog titled, "Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response," it became SEI’s most visited post of the year after only two days, according to a spokesman for the institute.

The desire for knowledge about DDoS is a welcome development, and it shouldn’t be limited to IT and security personnel.

"While DDoS attack prevention is partly a technical issue, it is also largely a business issue," said Rachel Kartch, analysis team lead at the CERT Division of SEI, a federally funded research and development center sponsored by the US Department of Defense and operated by CMU, and author of the DDoS post.

In general, organizations should begin planning for DDoS attacks in advance, Kartch noted in the post. "It is much harder to respond after an attack is already under way," she said. "While DDoS attacks can't be prevented, steps can be taken to make it harder for an attacker to render a network unresponsive."

To strengthen resources against a DDoS attack, it's important to make the architecture as resilient as possible, Kartch said. "Fortifying network architecture is an important step not just in DDoS network defense, but in ensuring business continuity and protection from any kind of outage or disaster situation," she said.

As part of this effort, organizations need to locate servers in their various data centers; and ensure that the data centers are located on different networks, have diverse paths, and have no notable bottlenecks or single points of failure.

"Overall, priorities for architecture should be geographic diversity, provider diversity, and elimination of bottlenecks," Kartch said. "While these are best practices for general business continuity and disaster recovery, they will help ensure organizational resiliency in response to a DDoS attack."

Another good practice is to deploy hardware that can handle known attack types and use the available features designed to protect network resources. "Again, while bolstering resources will not prevent a DDoS attack from happening, doing so will lessen the impact of an attack," Kartch noted.

Read the rest here:
http://www.zdnet.com/article/here-are-some-best-practices-for-preventing-ddos-attacks/
ISSA Photos are courtesy of our Chapter Photographer Warren Pearce.
The Information Systems Security Association (ISSA) is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?
If you would like to submit an article...

Do you have something that the Colorado Springs ISSA community should know about? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at:

doncreamer-issa@q.com

Ensure that “Newsletter” is in the subject line.
Looking forward to seeing you in print!

Seeing 100 Metronomes Synchronize on Their Own Is Awesome

By Casey Chan, Gizmodo, December 27, 2016

The machines are coming for us and we can’t pretend like we didn’t see it coming, because even the lowly metronome has been trying to warn us for years. Here are 100 of those ticking boxes starting at different beats but then slowly synchronizing themselves toward the same beat. It’s like they’re all being controlled by the same mind.

What’s happening is not exactly magic but is still pretty cool: the metronomes are transferring energy to the platform they’re on, which then transfers that energy back to the metronomes—until they all sync up and start hitting the beat in one glorious wavelength.

Read the rest here:

http://sploid.gizmodo.com/seeing-100-metronomes-synchronize-on-their-own-is-aweso-1790536767