THE DIR CYBERSECURITY INSIGHT

June FY2016 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

InfoSec Academy News

The OCISO is excited to announce we're re-opening the InfoSec Academy! Starting in June, the InfoSec Academy will include multiple libraries of courses and several delivery options.

Students will have access to Information Security and Business Skills course libraries via the OnLine Anytime (OLA) delivery method. These are computer-based training courses that students can access anytime from anywhere and complete on their own time. Most certification preparation courses will also be offered in this format.

In addition, certification preparation courses will be offered in an OnLine Live (OLL) format. OLL training is a hands-on training experience with a live instructor. Students can participate in discussions with the instructor and other students by voice or through the text-chat window using the Adobe Connect platform. Within the class, you will be able to:

- See the instructor's lecture slides, ask questions and provide feedback
- Work in virtual labs, just like in a traditional instructor-led class
- Hear and communicate with the instructor and other students
- Attend the class from your office or from a New Horizon's location

Students must take the Texas Security Policy and Assurance course before taking any certification prep course. If you took the class during the previous InfoSec Academy, you will receive credit for the course. The Texas Security Policy and Assurance course will be offered via the OLA format and through Instructor Led Training (ILT). We are working to offer the first of these ILT classes in late summer.

Here is a summary of the course offerings and available delivery methods:

OLA Training

- Business Skills Library
- Information Security Course Library
- Most Certification Preparation Courses
- Texas Security Policy and Assurance Course

OLL Training

- Certification Preparation Courses
  - Certified Information Systems Security Professional (CISSP®)
  - Certified Information Security Manager (CISM)
  - Certified n Risk and Information Systems Control (CRISC)
  - CompTIA Security+
  - Certified Ethical Hacker (CEH)

ILT Training

- Texas Security Policy and Assurance Course

For questions about the InfoSec Academy, including registration, please contact infosecacademy@dir.texas.gov.

CONTENTS

Network Security Operations Center (NSOC)

Since February 2015, the DIR NSOC team has been adding security alerts into the SPECTRIM (formerly known as Archer) incidents application. Agencies have been quick to respond and acknowledge these time sensitive alerts. This process has enabled improvements for agencies, the NSOC security team and allowed for better tuning of the NSOC security tools. We appreciate your continued support in this endeavor.

The NSOC security team also receives other types of security information from a diverse set of sources that may not rise to the level of a standard NSOC alert. The devices in place can detect alerts for smartphones. Most of these alerts are most likely for personal devices or public Wi-Fi networks and not internal devices. In the past, alerts were deemed unactionable and notifications were not sent out. However, after discussion with our ISO/CISO community it was discovered that customers would still benefit from receiving this information.

In May, the NSOC team began sending less critical alerts with the title "Informational Notification." They will continue to be entered into the SPECTRIM incident application to allow tracking and reporting. Because these notifications are not as time-sensitive, they will be tracked differently than standard NSOC security alerts. If for some reason the notification elevates to the level of a security incident, you can mark the incident as "confirmed" and continue to work the incident in SPECTRIM.

NSOC Informational Notifications categories currently are:

- Mobile Device (e.g. Android malware beaconing, etc.)
- Observed traffic on open ports/protocols that the NSOC cannot take action on, other than blacklisting the source IP. This stops the connection attempt from the identified IP once the block is in place, but doesn't necessarily prevent this type of activity in the future
- P2P ex. BitTorrent and TOR (even though we block TOR exit nodes at the NSOC Intrusion Prevention System, hosts may still be running the TOR client)
- Adware/Spyware commodity toolbars and browser hijacks.

Please email NSOC with any concerns or questions.

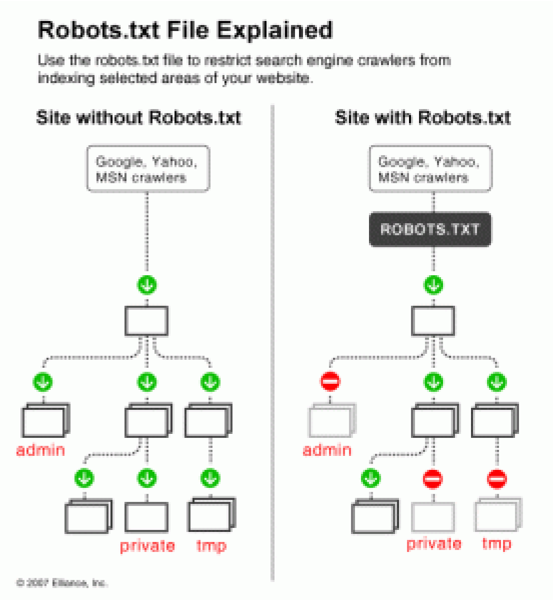
SPECTRIM

We will be adjusting the permission groups in SPECTRIM. In the past, there were different groups for incident and monthly incident reports. We will be combining all groups for incident giving users access to both the monthly and individual incident module.

REMINDER: Enter your cybersecurity funding requests into the Cybersecurity/Legacy Modernization application in SPECTRIM. Last session's appropriation bill, HB 1 Article IX, Section 10 requires DIR to submit a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems, as defined in the October 2014 Legacy Systems Study, to be considered for funding to the Legislative Budget Board by **October 1, 2016**. In order to be included in this prioritization, agencies must submit information about their requests to the department through the SPECTRIM online application. Find additional information including a webinar recording that presented this function.

Controlled Penetration Tests

Web robots (aka internet bots, WWW bots, crawlers, wanderers and spiders) are automated software programs tasked with recursively traversing websites in order to retrieve, analyze and file information. Though primarily used for indexing, web robots can be an invaluable tool for link validation, HTML validation, change monitoring and website mirroring. It may seem like web robots are very complex (and they can be), but they're usually just simple and structurally-repetitive scripts.


Robots.txt File Explained
Use the robots.txt file to restrict search engine crawlers from indexing selected areas of your website.
Site without Robots.txt
Site with Robots.txt
Google, Yahoo, MSN crawlers
Google, Yahoo, MSN crawlers
ROBOTS.TXT
admin
private
tmp
admin
private
tmp
© 2007 Elliance, Inc.

The most common web robots are search engine bots, or web crawlers, primarily used to index web content. What these web crawlers essentially do is visit a website, follow the links it contains, log what it finds and report that information back to a search engine database. They help search engines run more efficiently by creating a roadmap of an entity's webserver.

Unfortunately, they also make it easier for attackers to collect information like email addresses and/or potentially learn the inner-workings of your server directory. By using web robots, a hacker can harvest information regarding your web server's restricted paths and even the kind(s) of technology found on your server(s). Their objective -- reconnaissance.

Administrators will usually setup their webservers with a robot.txt file. These files set certain ground rules as to where a web robot can, or cannot, traverse. However, this tells hackers where to look by telling them where you don't want them to look.

You can set your robot.txt file to **Disallow** web robots from visiting any pages on your website. And this is generally fine for keeping out basic web robots. Of course, attackers have the benefit of writing their own web robots that can be directed to ignore a webserver's robot.txt file altogether.

So how do we combat a rogue web robot that's intent on gathering information? The first suggestion is to not use a robot.txt file to hide network information. It's best not to advertise a restricted area on your network than to plant a *metaphoric* red flag. Second, use password protection on your server directories to protect private URLs from showing up on search results. If rogue web robots are originating from a specific IP address, they can be blocked using network firewalls or server configurations. If the web robot is part of a larger network, like a *botnet*, then it's best to use advanced firewall rules to block IPs that attempt to make multiple connections.

If you're interested in learning more about web robots, I encourage you to visit http://www.robotstxt.org/.

Information Security Officer Spotlight

Dale Harville
Information Security Operations Officer
Texas Department of Banking

I am the Information Security Officer (ISO) for the Department of Banking (DOB). Prior to coming onboard with the DOB in June of 2014, I worked in higher education for 27 years. My last post was the Network Manager and ISO at Texas A&M University San Antonio.

Tell us how information security has changed since you started in your role.

The most we had to worry about in the late 80s was making sure everyone had a password and the door was locked. Now almost everything is hackable, including our appliances and automobiles.

As a society, most people are still in denial that they will fall prey to cybercrime. As an industry, I think we all understand the mission but not necessarily how to do it. Cybercrime is evolving faster than we are adapting to the new threats and our play books are outdated before we write them.

Who are your customers, and what is one of the most challenging areas for you?

My users/customers are the agency employees. I focus on keeping them safe and secure while they do their jobs out in the field.

What do you like best of your job?

Every day is something new. Just when I think I have a handle on current events, some bad guy tries a new tactic to attack us.

Have you ever changed career paths?

When I graduated from high school, I went into the U.S. Navy as a diesel mechanic. I also served as a firefighter and learned how to maneuver a landing craft. When the Navy moved to gas turban engine, most of us diesel mechanics were discharged.

What are your hobbies?

Working in my yard and genealogy.

Where did you grow up?

My youth before the 6th grade was in spent Clovis, NM and the Earth, TX area. Beginning in the 6th grade I lived in Lubbock until I joined the Navy.

Tell us about your most proud accomplishment.

I think my greatest accomplishment is supporting my family while my wife and three daughters earned their master's degrees. I also worked full time while I earned my master's degree.

People would be surprised to know that you…

I have been bitten seven times by rattle snakes and six times by scorpions. I had a very fearless childhood.

What is your favorite travel spot?

I rent a barge house in England and travel up and down the river systems with my wife.

If you could interview one person (dead or alive) who would it be?

Steve Jobs - I met him once when I was getting my Apple Certifications.

If you had to eat one meal, every day for the rest of your life, what would it be?

Mint chocolate chip ice cream.

Security Corner – Getting to Know the Team

Joe Poole
Lead IT Security Analyst
Department of Information Resources

What is your responsibility in DIR and with the State?

I am the lead security analyst for the DIR NSOC security team. We are responsible for providing perimeter security for the State of Texas networks. We monitor all traffic, looking for suspicious or malicious activity, alert the agency of the traffic so they can remediate the issue and protect the state agencies from bandwidth saturation DDoS attacks. In addition, much of our time is spent gathering intelligence on active malware campaigns, the latest political happenings and social causes and the actions of foreign governments. All of these translate into a variety of attacks on state assets against which we defend.

When and where did you start your career?

I started my IT career in 1990 as a VAX Operator for Motorola. I then became the IT Director at the Texas Association for REALTORS. I was later hired by the Texas Attorney General to be the digital investigator for the Consumer Protection Division. I loved the opportunity to use my diverse IT experience and knowledge to actually stop internet fraud. I also found out I have a bit of a criminal mind which helped me a great deal in tracking down web-based con men.

During my time at OAG, I met several members of the DIR security team. One day they asked what I did in my role. When they found out, they took an interest in my skills. I later ran into them and they told me they had posted a job that they thought would be perfect for me. I love what I do now. It is fast paced and at times a bit stressful, but the rewards are immediate and very satisfying.

What is your personal back ground?

I am a fifth generation Texan born and raised on the Texas coast in Victoria. I went to University of Texas as a Petroleum Land Management major. I left before completing my undergraduate studies to work in the family oilfield construction company. I got married and started a family shortly thereafter. I have three kids and five grandchildren.

What is the greatest lesson you have learned?

Don't sweat it! Worrying and getting stressed over everyday life doesn't accomplish a thing. Do what you can do. Take action or live with it. It really is that simple.

Do you have a favorite hobby or pastime?

Being outdoors! I have been a professionally sponsored kayak angler since 2009. I work boat shows, give kayak fishing seminars, work with the manufacturer to design and test new models. I was one of the first All Water Paddles guides in the Texas. I am also a TEEX certified Outdoor Wildlife Guide, ACA certified Paddle Instructor and ACA certified Coastal Expedition Leader. When I am not kayak fishing, I am either camping or playing disc golf. I spend a lot of time with my Great Pyrenees mix rescue dog, Miel. She travels with me and is a great disc golf & camping companion. If I could just get her to go in the kayak with me when I fish. But that ain't happening….

What do you like best about working at DIR?

I have the sweetest security job in the world. My customers are security and/or network professionals and they understand exactly what my team is communicating and typically know what they need to do to correct the issue. It is a team-oriented relationship and works well. I like interfacing with all the agencies and seeing the accomplishments as a result of teamwork. And with my criminal mind, I just love playing the game with the criminals, hacktivists, and nation/state actors.

Insight from our Texas CISO

Eddie Block
CISO, State of Texas

Ah… summertime. School is out, pools are open and the family station wagon is packed for that cross-country adventure to Wally World. It's a great time to let go of your cares and bask in the sun.

Unless, of course, you are in security. Then summer is the time when crazy kids are out of school, bored, with a computer, the heat plays tricks on electronics, critical data is left on a laptop in the backseat of a black car in a parking lot with no AC and anyone in the organization really could be locked out of their account while travelling.

OK, maybe I'm just a curmudgeon. Maybe I'm jealous of those kids that get to sleep late and eat cereal for lunch. However, it is important to remember that the threats continue even when the sun is shining and the lakes are full.

Ransomware has grown exponentially over the past couple years. Phishing is still the primary vector for data thieves. Hacktivism and DDoS attacks are still targeting governmental entities. None of these threats will go on vacation, in fact DDoS attacks may spike over the summer while colleges are on break. We all want to go to Schlitterbahn and enjoy some funnel cake with the kiddos, but we need to make sure that we have locked the doors and checked the windows before we leave the house.

I'm very lucky at DIR. I am part of an excellent team, who has been profiled in this newsletter over the past several months. I know I can take some time away and feel secure knowing they can carry on without me. We've cross trained, backed each other up and supported each other over the past year. We should not have a single point of failure within the organization with regard to our people. This effort not only pays dividends during the summer, but is valuable anytime someone on the team is sick, has a family event, or just needs time away. It is essential to the success of the business that employees remain engaged in the mission, in themselves and in their team.

As I've done for several years, this summer I will go to Las Vegas for Defcon (and lately B-Sides Las Vegas). The research, tools and vulnerabilities that are disclosed at these conferences are truly amazing. The talent and intelligence of the attendees always reminds me why I enjoy security in the first place. It is a way to "recharge" my security batteries. Taking some time to relax, and knowing that the home front is protected is a blessing.

So enjoy the benefits of Texas in the summer: fresh peaches, tubing, SeaWorld, Schlitterbahn, camping, rock climbing or whatever helps you recharge. Just remember bad guys aren't going on vacation, so stay vigilant.

Happy summer from your friendly, neighborhood curmudgeon.

Eddie Block
CISO, State of Texas

Events

2016 Save the Dates

- DIR Webinar to discuss the Gartner research licenses – June 6 at 11:00
- Monthly Gartner Webinar– June 21, at 10:00
  ”Get Me a Secure Line! – Protecting Communications with Voice and Texting Encryption”
- 2016 TASSCC Annual Conference: August 7 – 10, Galveston, TX
- 2016 NSA Information Assurance Symposium (IAS): August 16– 18, Washington, DC