NSF Division of Polar Programs, Arctic Sciences Section

Information Security 101

June/July 2014 Issue 5

Points of Interest:

- Tips for Protecting Your Systems & Research
- Security Learning Corner: Major IT Vulnerabilities in the News
- Google+ "Fraudulent Verification Survey"

Inside this issue:

Expectations for Awardees

Principal Investigators planning to work in the Arctic under an NSF grant should ensure that all field team members understand NSF expectations when using NSF sponsored IT system and services.

- Limit use of bandwidth to activities required for conducting and supporting research. Respect your fellow researchers by appreciating that bandwidth is a limited and costly resource at remote Arctic locations.
- Follow ARC Information Security Rules of Behavior, available on the NSF website. The Rules of Behavior details responsibilities of and expectations for all ARC Program participants that have access to ARC IT resources, including IT systems, infrastructure, services, and information.
- Be familiar with ARC information security policy and guidance available on the ARC RSL homepage on the NSF website (http://www.nsf.gov/geo/plr/arctic/res_log_sup.jsp).
- Be familiar and compliant with the HIPPA privacy rule and protect any medical information shared accordingly
- Recognize and protect personally identifiable information (PII) you are entrusted with, including your own information. Prevent inappropriate access, use, or disclosure by using appropriate protections when storing, transporting, transferring, e-mailing, remotely accessing, downloading, or disposing of sensitive information. PII includes:

  (i) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, passport number, date and place of birth, mother's maiden name, or biometric records.

  (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Tips for protecting your systems and research:

- Protect your IT systems on and off ARC sponsored networks by enabling auto-updates for antivirus and operating system software, and routinely patch all software applications.
- Restrict access to and closely monitor home institution systems connected to systems at remote Arctic locations.
- Only open email attachments that you are expecting to receive from a known entity.
- Backup data frequently and store backups on external media that is not connected to the primary data collection system.
- When sharing and storing data in the 'cloud', review and understand how data is managed and secured by cloud-computing service providers. Have your own data recovery strategy to ensure your data is not at risk if the service provider should experience a failure.

Security Learning Corner: Major IT Vulnerabilities In the News

The Heartbleed Bug

In April, one of the biggest security threats the internet has ever seen, an encryption flaw called the Heartbleed bug was uncovered. The flaw exists in Open Secure Socket Layer (SSL) software used to secure and encrypt most web communications.

An estimated two-thirds of all of the world's web servers use OpenSSL, the software behind most HTTPS sites that collect personal and financial information. The vulnerability compromises secret keys used to identify service providers and encrypt traffic (such as credit card numbers, user name and passwords), allowing for eavesdropping, impersonation, and data theft from both users and service providers. Major companies and websites affected include Google, Yahoo, Etsy, Netflix, Airbnb, NASA, Heathcare.gov and Amazon.

Major companies, banks and email services providers affected have since installed the latest version of Open SSL, but this flaw has existed for two years, so a breach or theft may have already occurred. Below are steps you can take to protect yourself from the Heartbleed bug:

- Compile a list of secure websites you usually use (banking, email, shopping etc.)
- Start with the most sensitive/critical and confirm the website or service has indeed installed/performed a security update in response to Heartbleed.
- After you've confirmed that the site or service has installed a security update, change your passwords.
- Keep an eye on your sensitive online accounts for suspicious activity.

For more information about Heartbleed:

http://www.defense.gov/news/newsarticle.aspx?id=122093

http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/

http://www.bostonglobe.com/business/2014/04/30/after-heartbleed-change-ocks/9gEdgfse8onY1dFCUxVszL/story.html

http://www.cnbc.com/id/101634780

Important:

Cyber criminals are working smarter and threats are increasing. Protect yourself by:

⇒ Keeping antivirus definitions and software up to date

⇒ Changing passwords to frequently used secure websites

⇒ Backing up data often and store offline

⇒ Do not download or open suspicious emails or files

⇒ For more information on email hoaxes and scams:

www.hoax-slayer.com

http://www.fbi.gov/scams-safety/e-scams

What Is Ransomware?

Ransomware is one of the newest types of malware vulnerabilities that is proving to be quite lucrative for cyber criminals.

Ransomware essentially kidnaps and holds users data hostage (usually by encryption) with attempts to extort money from these users in release of the kidnapped information. If users do not pay the ransom within a set timeframe, all captured data is deleted.

The Boston police department fell victim to (and was extorted) by the cyber criminals behind the CryptoDefense malware. Hackers reportedly made $34k in the first month the malware was released.

Ways to protect yourself from Randsomware:

- Back up your data often (and store this backup offsite/offline)
- Do not download, or open, suspicious email or click on files or suspicious links sent via email
- When doing business with reputable companies log into the company website to conduct business rather than clicking on links or opening attachments to emails.

For more information on Ransomware:

http://www.forbes.com/sites/sungardas/2014/04/21/how-to-protect-your-company-from-ransomware/

http://www.baselinemag.com/security/new-ransomware-is-as-dangerous-as-cryptolocker.html

Greenland Security & Contingency Planning Visit

Heather Fiebing of the ARC Information Security Team will visit Kangerlussuaq and Summit Station, Greenland July 14-22, 2014 . Goals for the visit include:

- Addressing Federal requirements for continuous monitoring & security control assessment (SCA)
- ARC IT & Communications (IT&C) Contingency Plan development and testing

To minimize the time required of on-site operations staff, the ARC Information Security Team works closely with IT&C service providers prior to the site visit to conduct interviews and gather supporting documentation and evidence. This approach results in a checklist of specific procedures and details that must be verified on site.

Security Control Assessment (SCA)

The SCA portion of the visit will evaluate a portion of the NIST SP 800-53 Rev 4 low baseline security controls on IT&C systems, services, and procedures supporting ARC operations in Greenland.

SCA activities include:

- Gather and document existing security practices of IT&C service providers
- Recommend policy, procedure or operational practice improvements to NSF ARC RSL Program Managers
- Identify how ARC Information Security Handbook policies are addressed,
- Identify recommended policy additions to the handbook based on feedback gathered on site.
- Assess risks in the case when sites, systems, processes, and procedures are not addressing ARC policies
- Work with IT&C service providers to document recommend mitigation approaches where risks are found.

When weaknesses are discovered by a security assessment, the GSS Vulnerability Remediation Action Tracker (VRAT) is used to plan activities for remediating the issue, and to regularly inform RSL Program Management of information security risks.

IT&C Contingency Planning

IT&C Contingency Plan development and testing activities include:

- Document roles and responsibilities, recovery objectives, and supporting procedures for IT&C systems required to support capabilities critical to ARC Greenland mission operations.
- Collaborate with CPS to conduct tabletop testing for a pre-defined set of key operational scenarios based on critical Greenland communications and processes.
- Draft an IT Contingency Plan that includes process improvement recommendations discovered through tabletop testing.
- Update the GSS VRAT where remediation actions are required to implement an effective contingency procedure.

Closing Remediated VRAT Items

Last but not least, site visits provide the opportunity for the ARC Information Security Team to verify closure of VRAT items for that operating location. If you plan to make changes to systems or procedures to address a VRAT item before the July visit, please inform Heather ahead of time to ensure the fix is confirmed while on site.

Contact Information

If you have any questions or concerns about the upcoming Information Security visit to ARC Greenland operating locations please email Heather Fiebing, ARC Information Security Lead (fiebing_heather@bah.com).

Google+ "Fraudulent Verification Survey" Phishing Scam

Phishers are again after Google account login details - this time they are trying pass themselves off as the nonexistent "Google+ All Domain Mail Team" and are urging users to participate in a "spam and fraudulent verification" survey:

The email threatens that if you don't participate in the survey your email account will be treated as a fraudulent user and be shut down.

If someone clicks on the link within the phishing email they are directed to a fake/spoofed Google login page.

If the user enters login information, these details are collected by the hackers behind the fraudulent email and used to either compromise the Google account or to send spam from that account, or the account information is sold to other criminals that will do the same.

"Phishing scammers often try to trick users into submitting login details and other personal information by claiming that account details must be verified to improve security," warns Hoax-Slayer.

If you are worried that this or a similar email might be legitimate and you might lose the account, please refrain from following the offered link, and access your account the usual way - via a bookmark or by typing in the correct address for the log-in page in the browser's address bar.

ARC Awareness & Training: Incident Response

Arctic Sciences Section Information Security Support is provided by SPAWAR Office of Polar Programs

Robert Myer, Program Manager, SPAWAR Office of Polar Programs (SOPP)
843.345.0800
robert.l.myer.civ@mail.mil

Sarah Wolfe Polar Program Manager
843.364.3350
wolfe_sarah@bah.com

Heather Fiebing Arctic Information Security Lead
303.221.0396
fiebing_heather@bah.com

Did you know?

Computer security incidents continue to rise. 2013 was the busiest year yet for cyber criminals. Our response to evolving threats includes:

- ARC Information Security Handbook revision (anticipated publication this Summer) to include the latest NSF and Federal guidance for handling IT Incidents.
- Arctic Program IT Incident Response instruction and procedures currently in development.

What is an IT incident?

An IT Incident is any activity that threatens confidentiality, integrity, or availability of information resources, has the potential to undermine science or operational activities, presents legal issues related to sensitive data, or is a misuse of government information resources. Examples include :

- Unauthorized access to ARC IT resources
- Prohibited use of ARC IT resources
- Breach of copyright laws
- Viruses, Worms and Trojan Horses
- Threats to individuals
- Unauthorized access or disclosure of PII or sensitive information, including paper disclosure, e-mail release or inadvertent posting of sensitive data on a public web site

Reporting a suspected incident

If while using an IT system provided by the Arctic program, such as Summit Station, Toolik Field Station, Barrow and other field sites, you suspect a potential security incident has occurred, immediately report information on the event to the site manager your CPS project manager, or one of the RSL program managers, Pat Haggerty or Renee Crain. If an incident occurs at your institution, please report it through your institution's IT office to protect other network users.

Reporting suspected incidents is a critical piece of the ARC incident response program, as the ARC is required to meet Federal incident reporting requirements by reporting suspected and confirmed incidents to NSF IT security authorities within specified time frames.

ARC IT Spotlight: Michael Lilly, CPS Head of IT

The ARC IT Spotlight is a new addition to the newsletter, to introduce and bring awareness of dedicated staff and services supporting ARC IT. For this spotlight we had the privilege of interviewing Michael Lilly, CH2M HILL Polar Services Head of IT.

Q: Michael, what is your favorite part of the job?

A: The people in this program are great to work with. Folks in the program put politics aside, and are open, collaborative, and focus on program and science success. I feel that supporting polar sciences is important, and I have a personal interest in contributing to the polar science mission.

Q: What is your professional background?

A: I am a long time IT engineering professional, who started in the field as a disk drive engineer in the 80s. I took a sabbatical to raise my twins for four years while going to school for computer science. I went to work for MCI in the mid 90s, followed by six years of supporting the USAP as a software manager for their business applications. I went to work at Unum Provident as Director of IT and was promoted to Vice President in 2008. I came to work at CH2M HILL in 2010 as an external IT consultant, and became a fulltime employee in March 2012. I began the Polar Services Head of IT position in January 2014.

Photo: Michael and his twin son Cameron and daughter Leanne at a Portland Timbers game.

Q: From a personal standpoint, what are you excited about these days?

A: I am excited about throwing a big celebration for my twins birthday this summer. We are bringing in lots of out of town friends and family and are looking forward to a fun affair. I am also always excited about my dogs, a 4 year old Pit bull, Chloe (who was rescued from dogfighting) and my 10 year old Labrador, Buddy.