Monthly Cybersecurity Newsletter

April 2017 Issue

Information Technology

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

---

Don't Lose Your Money at the ATM

People go to an automated teller machine (ATM) because they want to withdraw money from their financial accounts, not to give information to someone else to steal their funds. Unfortunately, it has become incredibly easy and common for thieves to steal other people's funds by attaching "skimming" devices to ATMs. ATM card skimmers contain electronics that store payment card data from the magnetic strip on a card. Paired with a miniature camera also attached to the ATM that records individuals entering their Personal Identification Number (PIN), thieves have the necessary information to fabricate new cards and to withdraw cash from victim accounts. The best way to protect yourself from ATM fraud is to inspect the card insert slot of a machine to make sure it is firmly attached. If the machine looks strange, find another ATM. Also, be sure to cover your hand as you enter your PIN. For more information about this topic, read the article "Why I Always Tug on the ATM" at https://krebsonsecurity.com/2017/03/why-i-always-tug-on-the-atm/.

The Threat from Inside

In September 2016, a boot-making company in El Paso, Texas decided to give one of their IT engineers…well, the boot. The company revoked the employee's access rights as he left the building. However, after a volatile exit from the company's facilities, the disgruntled ex-employee took revenge on his former employer by shutting down the company's email server and their application server that ran the main production line. The individual had used a hidden administrator account that was disguised to be an innocuous service account with full administrator privileges that were not needed. After three hours of troubleshooting, the company was forced to send 300 employees home. They also had to hire an outside contractor to help fix the damage from the incident. It took the company weeks to catch up on lost orders and production. As a result of the incident, the company claimed to have lost $100,000 in new orders plus the cost of hiring additional help to restore the company's system.

Insider threats are a big problem! Did you know: 28% of electric crime events were known to be caused by an insider threat? 46% of the costliest cybercrime events were a result of an insider

threat. 34% of insider threat cases targeted collecting personally identifiable information (PII). While the perpetrator of the aforementioned incident was caught, it is a reminder of the importance to audit all system accounts, to know their function and access, and to be sure that all accounts have only the access necessary to perform their function(s). For more information about insider threats, be sure to review the **Insider Threat Tip Card** at the end of this newsletter.

Remember, there are other monthly newsletters available to you that contain a wealth of information! The following are the various cybersecurity newsletters the ESRMO distributes each month. These newsletters contain information we hope you find beneficial.

SECURITYsense Newsletter: A licensed monthly newsletter that contains several articles that are usually relevant to current cybersecurity issues.

https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/SECURITYsense

Disclaimer: The SECURITYsense newsletter is a licensed product of the National Security Institute, Inc. (NSI) and is protected by the United States copyright laws. Distribution via an open Internet site (available to anyone with Internet access), Extranet, or other public access network is strictly prohibited.

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's topic is titled ***Digital Spring Cleaning.***

http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-tips-newsletters

SANS OUCH! Newsletter: A free monthly information security awareness newsletter provided by The SANS Institute. This month's topic is on ***Passphrases***.

http://securingthehuman.sans.org/resources/newsletters/ouch/2017

Did you know that The SANS Institute also provides *free* awareness **videos** and **webcasts**? The SANS Video of the Month may be accessed at https://securingthehuman.sans.org/resources/votm.

Also, The SANS Institute offers free webcasts on a variety of topics that may be accessed at https://www.sans.org/webcasts/upcoming.

Business Continuity Awareness Week (BCAW) 2017 will be held **May 15th – 19th, 2017**, and the theme for the week will be *cyber resilience*. To raise awareness on this important topic, the ESRMO will be sending out business continuity awareness briefs each day during BCAW.

Don't forget about the following upcoming training opportunities that are available through the statewide Learning Management System (LMS).

- **April** – Information Protection: Protecting Information (**Due:** 5/16/2017)
- **June** – Computer Security: Don't Let Your Computer's Defenses Down
- **August** – Mobile Security: Mobile Devices – The Future is Now
- **October** – Public Wi-Fi: Be Careful Out There
- **December** – Office Security: Keeping Your Office Secure

If you have questions about the training schedule or the training content, please contact Maria Thompson, State Chief Risk Officer, at maria.s.thompson@nc.gov or at (919) 754-6578.

The NC Office of the State Controller (OSC) is promoting the following E-commerce/PCI Data Security Standards educational opportunities with the help of Coalfire:

- **June 20** at 10:00am – What is P2PE Encryption?
- **August 15** at 10:00am – What is a Physical Security Assessment and Benefits?
- **October 24** at 10:00am – Implementing an Effective Employee Security Training Program

Each webinar will last approximately **1 hour**. Additional information for each of the webinars, along with a registration link, will be distributed a few weeks prior to each scheduled event.

Other important events coming soon…

- **September 1, 2017** – Agency Compliance Reports due!
- **October, 2017** – National Cyber Security Awareness Month

---

Cybersecurity and Risk Management Site:
http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management

Cybersecurity Awareness Page:
https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness

ESRMO SharePoint Site:
https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/default.aspx

State of NC Cybersecurity Incident Reporting Site:
https://it.nc.gov/cybersecurity-situation-report

Do you have something to share? Is there a topic you think we should cover in a future newsletter? We encourage all security professionals to send us topics that will be of value to other agencies in order to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider including it in a future newsletter, please send it to security@its.nc.gov.

INSIDER THREAT TIP CARD

We often think of cyber threats as coming from an anonymous criminal, hundreds of miles away behind a computer screen. However, current and former employees who have intimate and valuable knowledge about a company are also capable of committing a cybercrime.

An insider threat occurs when a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data, intentionally misuses that access in a manner to commit a cybercrime.[1]

DID YOU KNOW?

- 28 percent of electric crime events were known to be caused by insider threats.[2]
- 46 percent of the most costly cybercrime events were a result of an insider threat.[3]
- 34 percent of insider threat cases were targeted towards collecting personally identifiable information (PII).[4]

TIPS TO MITIGATE INSIDER THREATS

Insider threats are a result of a combination of organizational, behavioral, and technical issues. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) recommends the following best practices for addressing these issues and mitigating an insider threat:

- Incorporate insider threat awareness into periodic security training for all employees.
- Implement strict password and account management policies and practices.
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
- Ensure that sensitive information is available to only those who require access to it.
- Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
- Develop a formal insider threat mitigation program.

BEHAVIORAL INDICATORS

A good way to prevent an insider threat is to train your employees to recognize some common behavioral indicators among their colleagues. US-CERT has identified the following behavioral indicators of malicious threat activity:

---

[1]The United States Computer Emergency Readiness Team (US-CERT)

[2] CERT and Carnegie Mellon University: "U.S. State of Cybercrime Survey", 2014.

[3] Ibid

[4] Carnegie Mellon University, "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector" 2012.

- Remotely accesses the network while on vacation, when sick, or at odd times during the day.
- Works odd hours without authorization.
- Unnecessarily copies material, especially if it is proprietary or classified.
- Expresses interest in matters outside the scope of their duties.
- Shows signs of drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health, or hostile behavior.

IF YOU'VE BEEN COMPROMISED

- Follow your organization's rules and regulations regarding cyber threats.
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.
- Inform local law enforcement as appropriate.
- Report stolen finances or identities and other cybercrimes to the Internet Crime Complaint Center at www.ic3.gov.
- Report fraud to Federal Trade Commission at www.FTCComplaintAssistant.gov

RESOURCES AVAILABLE TO YOU

US-CERT.gov

Report incidents, phishing attempts, malware, and vulnerabilities computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.

IC3.gov

If you are a victim of online crime, file a complaint with the Internet Crime Compliant Center (IC3) at www.ic3.gov.

FTC.gov

Report fraud to the Federal Trade Commission at www.ftc.gov/complaint.

Stop.Think.Connect. is a national public awareness campaign aimed at empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family and your community. For more information visit www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™