Monthly Cybersecurity Newsletter
December 2017
Issue

Enterprise Security and Risk Management Office (ESRMO)

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

Don’t Take The Bait!

Phishing emails continue to be a significant risk to systems and data. For instance, Mecklenburg County was the victim of a recent phishing attack. County systems were compromised when one or more employees inadvertently opened a phishing email – a message that appears to come from a trusted source but actually contains a malicious link or attachment. Authorities believe attackers used a compromised employee account to send a phishing email to other staff that when opened allowed ransomware to encrypt the county’s systems. The ransomware attack demanded $23,000, which county officials refused to pay. Instead, the county began the arduous task of restoring its systems using back up data. This incident shows us that even though an organization spends millions of dollars to secure its systems and data, a person clicking on one malicious link in an email can compromise its systems and data.

Phishing attacks used to be easier to spot because they included grammatical and spelling errors, and links to phony web sites. However, phishing messages are becoming increasingly harder to spot. For instance, more phishers are using SSL certificates (e.g. HTTPS) in order to increase the likelihood users will trust that the site is legitimate. The average Internet user has been taught for years to simply “look for the lock icon” in the browser address bar to ensure a site is safe. That is no longer true. What steps can you take to avoid becoming the next victim?

Be leery of unexpected messages and attachments: Do not open attachments in emails you were not expecting, even if they appear to come from someone you know.

Don’t take the bait: Most phishing attacks try to convince you to act quickly to avoid some kind of loss, cost or pain. Emails that emphasize urgency should be considered extremely suspect.

Links Lie: Don’t trust that a link will take you where it says it will go. Always hover over a link with your mouse to see where it will actually go. Better yet, it is safer to not click links in an email message. Manually type the web address or use a known good bookmark to access a site.

“From” Fields can be spoofed: Just because a message appears to be sent by someone you know, doesn’t mean that it was. This information can be and frequently is spoofed.

Ask for confirmation: If a message seems suspicious and asks for a response, call the sender using a known phone number that did not originate from the suspicious email – like your personal address book or the “contact us” page on a legitimate website.

Preventing 85% of Cyber Attacks

You have heard it said: *an ounce of prevention is worth a pound of cure*. If we take certain precautions, we can reduce the likelihood of problems later. This is true for cyber threats, as well. While we cannot prevent every possible threat, there are things we can do to greatly reduce the risk of a cyber attack. The Department of Homeland Security (DHS) encourages organizations to implement the following items, which they claim can prevent as much as *85 percent* of targeted cyber attacks.

- *Patch applications and operating systems* – Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of vulnerabilities that an attacker can exploit.
- *Application whitelisting* – Whitelisting is one of the best security strategies as it allows only specified programs to run while blocking all others, including malicious software.
- *Restrict administrative privileges* – Limiting who has admin privileges to a system may prevent malicious software from running or limit what it can do and spreading elsewhere.
- *Input validation* – Input validation is a method of sanitizing untrusted user input provided by users of a web application. This may prevent many types of web application security flaws, such as SQLi, XSS, and command injection.
- *Firewall configuration* –Firewalls can be configured to block data from certain locations or applications while allowing relevant and necessary data to pass through.

While the above strategies may be common sense, DHS continues to see intrusions because organizations fail to implement these basic measures. They tell us that a commitment to good cybersecurity and best practices is critical to protecting systems. The following are some questions you can ask to help reduce the risk of attack to your organization's data and systems:

- *Backups*: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
- *Risk Analysis*: Have we conducted a cybersecurity risk analysis of the organization?
- *Staff Training*: Have we trained staff on cybersecurity best practices?
- *Vulnerability Scanning & Patching*: Have we implemented regular scans of our network and systems, and appropriate patching of known system vulnerabilities?
- *Application Whitelisting*: Do we allow only *approved* programs to run on our networks?
- *Incident Response*: Do we have an incident response plan, and have we practiced it?
- *Business Continuity*: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
- *Penetration Testing*: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

DHS offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of these resources, visit https://www.us-cert.gov/ccubedvp.

Don't forget…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 involving 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 edition is on ***Avoiding Holiday Scams***.

https://www.cisecurity.org/resources/newsletter

- **SANS OUCH! Newsletter:** A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Lock Down Your Login.***

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.

The final security module for 2017 through the statewide **Learning Management System (LMS)** is *Office Security: Keeping Your Office Secure*. This course is designed to meet the 2017 annual cyber awareness training requirement for all State employees.

Note: *Agencies need a minimum 90% completion to be compliant.*

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

FEDERAL VIRTUAL TRAINING ENVIRONMENT

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at no cost to government staff, including contractors. With 60+ courses at varying levels of proficiency – from beginners to advanced – all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated on a rolling basis.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ Over **60+** available courses of varying proficiency – beginner to advanced
- ✓ Self-paced
- ✓ Many popular certification courses including:
    - Network +
    - Security +
    - Certified Information Systems Professional (CISSP)
    - Windows Operating System Security
    - Certified Ethical Hacker (CEH)
- ✓ All courses are aligned to the NICE Cybersecurity Workforce Framework
- ✓ Individuals can take courses to build the required knowledge, skills, and abilities in the cybersecurity field
- ✓ Taught by experienced cybersecurity subject matter experts

For more information and to visit FedVTE, please go to https://fedvte.usalearning.gov.

Upcoming Events…

- ➢ **January 1, 2018** – New Year's Day Holiday
- ➢ **January 15, 2018** – Martin Luther King Jr. Birthday
- ➢ **January 28, 2018** – Data Privacy Day
- ➢ **January 30-31, 2018** – *NIST Risk Management Framework* training @ 3900 Wake Forest Rd., Raleigh NC.
- ➢ **February 20, 2018** – Quarterly Security Liaison Meeting

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all 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 for a future newsletter, please send it to security@its.nc.gov.