Monthly Cybersecurity Newsletter

January 2023 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the Interim State Chief Risk Officer – Carly Sherrod

Cybersecurity Experts Weigh in on Modern Email Attacks

Abnormal Security's chief information security officer, Mike Britton, shares the best advice from a three-part webinar series on the current state of risk in email-based cyberattacks. The threat of email attacks today is so great that it took Abnormal Security three separate webinars to cover it. In a recent blog, Britton provides the highlights and major takeaways and brings you nuggets of wisdom that can have real impacts on your cybersecurity strategy's focus and execution for stopping email-based attacks. A few of the pearls pulled from that article are that:

- Modern threat actors do extensive research on their targets, creating convincing emails that trick employees.
- Compromised credentials (a focus of most phishing campaigns today) provide threat actors with the ability to access other applications, let them reset passwords for other accounts and can serve as the basis for launching additional attacks.
- Email will continue to be a primary attack vector for ransomware because of the breadth of abilities threat actors have to trick recipients into opening attachments.
- Stopping attacks is a shared responsibility. Troy Hunt (of *Have I Been Pwned?* fame) said that "requiring employees to complete ongoing security awareness training can help them identify malicious emails that are usually the first step in attacks."

Take a look at the longer list of key takeaways, and realize that anytime email is involved in an attack, so are your users – making it necessary to enroll every one of them in security awareness training so they can play their part in stopping email-based cyberattacks.

This article is redistributed with permission from KnowBe4.

CISA Releases Phishing Infographic

The U.S. Cybersecurity and Infrastructure Security Agency has published a phishing infographic to help protect both organizations and individuals from successful phishing operations. It provides a visual summary of how threat actors execute successful phishing operations. Metrics compare the likelihood of certain types of "bait" and how commonly each bait type succeeds in tricking the targeted individual. The infographic also provides detailed actions organizations and individuals can take to prevent successful phishing operations – from blocking phishing attempts to teaching individuals how to report these incidents. View the infographic.

CISA, NSA and ODNI Release Guidance for Customers on Securing the Software Supply Chain

The U.S. Cybersecurity and Infrastructure Security Agency, National Security Agency and Office of the Director of National Intelligence published the third of a three-part series on securing the software supply chain: Securing Software Supply Chain Series - Recommended Practices Guide for Customers. This publication follows the August 2022 release of guidance for developers and October 2022 release of guidance for suppliers.

The released guidance, along with the accompanying fact sheet, provides recommended practices for software customers to ensure the integrity and security of software during the procuring and deployment phases.

The Securing Software Supply Chain Series is an output of the Enduring Security Framework, a public-private cross-sector working group led by NSA and CISA. This series complements other U.S. government efforts underway to help the software ecosystem secure the supply chain, such as the software bill of materials community.

CISA encourages all organizations that participate in the software supply chain to review the guidance. See CISA's Information and Communications Technology Supply Chain Risk Management Task Force, ICT Supply Chain Resource Library and National Risk Management Center (NRMC) webpages for additional guidance.

Join NCDIT for Data Privacy Week Jan. 22-28

In observance of Data Privacy Week, the N.C. Department of Information Technology is holding two lunch-and-learn webinars for state employees.

Monday, Jan. 23 (Noon to 1 p.m.)

Chief Privacy Officer Cherie Givens will share why privacy matters and how you can better protect personally identifiable information at work and at home.

Learn also how the state is prioritizing privacy and data protection as it works to serve the people of North Carolina. Topics will include:

- What privacy is and why it is important
- Privacy encompasses data protection
- How state employees protect privacy
- Tips to protect your privacy at home

Sign up for the Microsoft Teams webinar at https://it.nc.gov/privacy-webinar.

Thursday, Jan. 26 (Noon to 1 p.m.)

Dive deeper into privacy with this panel discussion. Ideal for agency leadership, CIOs, privacy points of contact, security staff and others, topics include:

- What the Office of Privacy and Data Protection is doing to support privacy in our state government
- How we work together to address privacy issues at the agency level
- What the privacy office does to help implement Privacy by Design/Privacy by Default
- Why we need more privacy champions in state agencies

Sign up for the Microsoft Teams meeting at https://it.nc.gov/deep-dive.

How to avoid **Social Engineering**

WENDY'S TIPS

1

Think before you Click!

Is the story really plausible?
Make sure that information is actually genuine, for example by calling back.

2

Don't let them pressure you!

Does something have to be done very quickly or are you being threatened with severe consequences?
Then be particularly wary!

Speak to others!

When something unusual happens, talk to members of your team. Ask again, especially for unexpected messages or phone calls.

3

4

Report incidents!

Even if you've spotted the scam, report it immediately. You might not be the only one being targeted by attackers.

exploqii

Cybersecurity Resilience Emerges as Top Priority as 62% of Companies Say Security Incidents Impacted Operations

Cisco's annual Security Outcomes Report shows that executive support for a security culture is growing. The report identifies the top seven success factors that boost enterprise security resilience, with a focus on cultural, environmental and solution-based factors that businesses leverage to achieve security.

A whopping 62% of the surveyed organizations shared that they have experienced a security event that impacted business in the past two years. Common types of incidents include a network or data breaches (51.5%), system outages (51.1%), ransomware events (46.7%) and distributed denial of service attacks (46.4%).

These incidents had harsh consequences for the companies that went through them, as well as the other businesses they worked with. The most common effects were IT and communication problems (62.6%), supply chain disruptions (43%), weakened internal operations (41.4%) and long-term damage to their reputation (39.7%).

The report findings reveal that security resilience was a top priority for 96% of surveyed executives. Furthermore, preventing incidents and mitigating losses were the main objectives related to security resilience for security leaders and their teams.

A few highlights:

- Organizations that reported poor security support from the C-suite scored 39% lower than those with strong executive support.
- Advanced extended detection and response capabilities correlated to an incredible 45% increase for organizations over those that reported having no detection and response solutions.
- Businesses that reported an excellent security culture scored 46% higher on average than those without.

It is loud and clear that an ounce of prevention is worth a pound of cure. Going through through security awareness training and enabling end users to easily report suspicious emails that can quickly be responded to are extremely efficient ways to improve your security culture.

More details and a link to the report are available on Cisco's blog.

This article is redistributed with permission from KnowBe4.

Training and Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note**: You must have a valid state employee Microsoft 365 account*.

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

Jan. 22 - 28: Data Privacy Week

Jan. 24: SANS Webinar: What Works in Reducing Compliance Costs and Increasing Resilience with Integrity Management Tools

Jan. 24: SANS Webinar: Protecting People is a Pillar of Cybersecurity: Five Steps to Effective Executive Protection

Feb. 9: SANS Webinar: What Works in Improving End User Phishing Awareness, Recognition and Resistance

Feb. 24: SANS Webinar: SANS 2023 Incident Response Solutions Forum

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember … Stop. Think. Connect.*

***Disclaimer**: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*