Monthly Cybersecurity Newsletter

July 2021
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 – Rob Main

Increased Cyber Attacks Require Increased Vigilence

According to new data from VMware Carbon Black's Global Security Insights Report 2021, the sophistication and impact of modern cyberattacks is causing chief information security officers (CISOs) to rethink how to secure their organizations.

According to the report, "the frequency of attacks is high, sophistication continues to evolve, and breaches are the inevitable result." Cyber attackers are getting more aggressive, more talented, and more successful. The following are some statistics from the report:

- 76% of CISOs said the number of attacks they face has increased in the past year
- 79% said attacks have become more sophisticated
- 81% have suffered a breach, with an average of 2.35 breaches experienced per organization
- 82% said they have suffered a material breach

When asked what is causing breaches, **three vectors of attack** were at the top: Third-party applications were the most common culprit, followed closely by ransomware, and then out-of-date security technology. The report called for organizations to prioritize improving visibility into all endpoints on an organization's network. This includes the ability to continuously monitor the security and use of applications. Security tools, software, and processes must also be kept current or replaced when no longer effective. Interestingly, the report stated that the increase in sophisticated threats is ***related*** to having a more remote workforce.

Regarding the ransomware threat, the report calls for organizations to "combine advanced ransomware protection with robust postattack remediation that detects the continued presence of adversaries in their environment." This solution seems to overlook one critical aspect of reducing the risk of cyber-attack: ***cybersecurity awareness and training***. If employees (remote or otherwise) are a factor in the increased cyber-attacks, then they need to be exposed to ***current and ongoing*** cybersecurity awareness training. While technology can and should be used to reduce the risk of cyber threats, every organization needs to implement, support, and regularly provide cybersecurity awareness training for their personnel, including phishing simulations, to reduce risk and improve cybersecurity.

For more information about tips for remote working and improving your cyber posture, be sure to read Cybersecurity Tips for Remote Working & Learning During COVID-19.

Cybersecurity Tips in the Age of Ongoing Attacks

Cybersecurity is oftentimes described as an onion. There is not a silver bullet that protects an organization's systems and data. There are, however, many layers of security that ought to be applied and pulled apart in order to reach the core. The following tips for basic cybersecurity hygiene are provided by Janus Associates, an IT security firm that provides cybersecurity assessment services.

- **External Penetration Testing** – Find out who can access your systems and network from the outside.

- **Web Application Testing** – Gain insight into whether your external facing applications are secure.

- **Patching** – Get your systems updated and make sure they stay current.

- **Anti-Virus & Anti-Malware Solutions** – Use a state-of-the-art solution and make sure they are configured correctly and fully updated.

- **Next Generation Firewalls** – If your firewalls are older than three years, consider replacing them with next-gen technology that screens inbound traffic and updates in real-time.

- **Incident Response Plans (IRP**) – If you suffer a cyberattack, you will need an IRP that works. If you have a plan, makes sure it reflects your current infrastructure and operations, and test it before you need it to make sure it is effective. If you don't have an IRP, ***create one now***.

- **Business Continuity Plan (BCP)** – A BCP is another must-have. It should take you step-by-step through the process of restoring your systems and operations in the event of a cyber incident. If you have a BCP, confirm that it is current and test it to make sure it works. If you don't have a BCP, don't delay in creating one. It is the difference between successfully restoring your operations or failing and possibly being crippled for an extended period of time.

- **Email Phishing Tests** – Understand who in your organization knows what to open and what not to open. Phishing simulations can provide a way to raise awareness before an actual threat is received.

- **Security Awareness Training** – This is a must for every employee in every organization. It should be mandatory for everyone. People forget cybersecurity and new attack vectors are created daily.

- **Designate a Chief Information Security Officer (CISO)** –The CISO oversees and is responsible for all data security operations and initiatives. If you don't already have a CISO, you need one, and if you can't afford one, consider a virtual CISO.

No system is completely secure, but applying the necessary layers of security can decrease the liklihood of a successful cyberattack. North Carolina state agencies that have questions about creating or updating an IRP or a BCP; would like more information about conducting phishing simulations; or have questions about enhancing their security awareness training, contact the N.C. Department of Information Technology.

To read the original article from Janus, visit here. Janus is one of several vendors on the state of North Carolina's Statewide IT Contract 918a that lists pre-approved vendors who provide security assessment services.

Zero Trust and the New Normal of Cybersecurity

With an unprecedented rise in cyberattacks, 2020 was an eventful year for cybersecurity. Many organizations were caught off guard as the COVID-19 pandemic accelerated and dictated the need for remote work and education. However, the accelerated move to everything cloud has left many wondering about the future, whether their on-premise investments have been rendered obsolete or if the "new normal" would only rely on cloud-only solutions.

The pandemic has also highlighted the need for fool-proof Zero Trust implementations to enhance the security of networks against modern cyberattacks, whether they are initiated from the outside or within. However, with most internet traffic encrypted, it is becoming increasingly difficult to effectively implement a Zero Trust approach.

The Information Systems Security Association (ISSA)® is providing a free on-demand webinar that discusses:

- What the "new normal" of cybersecurity might look like in a post-pandemic world
- What role Zero Trust will play in the future of cybersecurity
- Why effective decryption is essential for a fool-proof Zero Trust implementation

To register for this free webinar, click here.

'PrintNightmare' Affects All Versions of Windows

On June 30, 2021, the Enterprise Security and Risk Management Office (ESRMO) shared information about a remote code execution vulnerability (CVE-2021-34527) in the Windows Print Spooler service that affected all versions of Microsoft Windows. The Windows Print Spooler service is a key operating system component that manages all printing on a Windows device. The vulnerability potentially allowed an attacker to gain elevated privileges on vulnerable systems.

Proof-of-concept code was proven effective against up-to-date and fully patched servers. At the time, the only known mitigation was to disable the Print Spooler service until Microsoft provided an effective patch to the vulnerbility.

The ESRMO sent another notification on July 7, 2021, regarding a newly released ***critical*** Microsoft security update for the Windows Print Spooler Remote Code Execution Vulnerability. Microsoft recommended that organizations apply this patch immediately after appropriate testing.

Public facing Windows servers are the highest priority for remediation; however, per security best practice and hardening requirements, unnecessary services should be disabled. The Print Spooler service is only required for Print Servers, so it ***should be disabled*** on all Windows servers except Print Servers.

For more information, please review the Emergency Directive (ED) 21-04 from the Cybersecurity and Infrastructure Security Agency (CISA).

Phishing Fundamentals

What Happens When You Click?

Like most scams, phishing leverages human emotions to trigger a response. The attacker wants you to do something against your best interests: click on a link, download an attachment, send sensitive information. They convince you to perform these actions by creating a fraudulent scenario, such as offering large sums of money, threatening you with late fees, or claiming that your account has been locked due to fraudulent activity. So what happens when you click on a phishing link? Here are just a few examples:

You have personal information stolen.

In a lot of cases, a phishing link will direct you to a webpage that looks legitimate. The page will ask you to enter various types of personal information like your full name, email, username, password, and so on. If you proceed, you effectively send that data to a criminal, who can use it to open fraudulent accounts in your name.

You lose control of your accounts.

Let's say you're logged in to your bank account when you click on a phishing link. This may allow cybercriminals to run an exploit known as session hijacking. Session hijacking allows them to intercept the communication between the bank's website and your computer and take control of your account. If successful, they will gain all the same access you have, allowing them to transfer money, change passwords, and steal personal data.

You infect your device with malware.

In more insidious phishing attacks, clicking on a link or downloading an attachment could result in malicious code that corrupts your device, steals data, or worse yet, infects your computer with ransomware. Ransomware is of particular concern here at work because it could encrypt our data or lock our systems until a ransom is paid, leading to both a loss in revenue and expensive downtime.

All of these scenarios are just examples of what could happen. Regardless of severity, falling for a phishing scam must be avoided no matter what.

How to Spot Phishing Attacks

To identify phishing attacks, carefully inspect the message and answer these questions:

- Are you familiar with the sender?
- Does the message contain poor grammar or misspelled words?
- Are there any suspicious links or unexpected attachments?
- Does the message offer unrealistic promises, like large sums of money?
- Does it plead with you to click on a link, download something, or send personal information?
- Does it threaten you by saying an account has been hacked or that you face legal action?

If you answered yes to any of those questions, then you've identified one or several red flags that the email is a scam.

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.
***Note**: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2021

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). https://www.cisecurity.org/resources/?type=newsletter

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

July 20: SANS Webinar: Are Cloud Service Provider Tools Enough to Secure Your Identities?

July 27: SANS Webinar: A SANS 2021 Report: Top New Attacks and Threat Report

July 27: RSAC Webcast: Modern Identity Hacking: Have Hackers Really Adjusted to Constant Remote?

July 28: CIS Webinar: Security Beyond the Perimeter - Accelerating Government's Journey to Zero Trust

July 30: SANS Webinar: Securing your Enterprise: Why Protection is Essential

Also, for a list of upcoming SANS webcasts, visit here.

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.*