Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare | TLP:WHITE | Alert ID : 0a041b71 | Oct 31, 2023, 08:27 AM

This week, *Hacking Healthcare*™ begins with a brief overview of the Cybersecurity and Infrastructure Security Agency's (CISA) announcement that they are updating the National Cyber Incident Response Plan (NCIRP). We briefly provide members with an overview of what the NCIRP is before discussing how it could be impactful to the healthcare sector and how members can become involved. Next, we review some new guidance, *Phishing Guidance, Stopping the Attack Cycle at Phase One*, jointly released by CISA, the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) on October 18, 2023.[i] We review the contents of the Guidance, discuss how it pertains to Health-ISAC members, and suggest several actions Health-ISAC members may hope to consider as a result.

Welcome back to *Hacking Healthcare*™.

CISA Begins National Cyber Incident Response Plan (NCIRP) Update

Earlier this month, CISA announced it had begun the work of updating the current NCIRP, which was published back in 2016, to better address the modern cyber threat environment and to better reflect significant changes to the U.S. government's organization. Let's dive into what this document is, how its revision may have significant implications for critical infrastructure sectors like healthcare, and how members can get involved in the revision process.

What is the NCIRP?

Very briefly, the NCIRP serves as a strategic framework for national coordination and response to significant U.S. cyber incidents. It outlines the roles, capabilities, and coordination structures for public and private sector entities and describes how the actions of all these stakeholders fit together to provide an integrated response. It also contains useful information in its annexes, such as the authorities and statutes that government entities are bound to, the schema for how significant cyber incident severity is assessed, and thoughts on information sharing. Some of these are particularly outdated at this time, but a revised version could be very helpful.

To be clear, the NCIRP is not for the everyday cyberattacks that may negatively impact a healthcare organization; it is meant to apply to cyber incidents "that are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[ii] For those interested in what that might look like, we would encourage you to consider participating in next year's Health-ISAC Hobby Exercise.

Why the Update?

The current NCIRP was released in December of 2016. While nearly seven years may not be an exceptional amount of time in law and policy circles, technology, the cyber threat landscape, the maturity of the private sector, and even the organization of the U.S. government have changed dramatically in that time. At its release, ransomware had yet to become the ever-present scourge of the healthcare sector, and neither CISA nor the Office of the National Cyber Director (ONCD) even existed. Needless to say, the current NCIRP doesn't adequately reflect today's realities in the U.S.

What is Changing?

While we might not know all the specifics until a draft is released, CISA's fact sheet has hinted at some aspects that need updating. This includes incorporating new entities like CISA and ONCD, updating the roles and capabilities of entities based on changes to authorities or cyber maturity, and ensuring the new NCIRP is more inclusive of non-federal stakeholders.

Action & Analysis
Included with Health-ISAC Membership

CISA, NSA, FBI, and MS-ISAC Release Phishing Prevention Guidance

According to CISA, more than 90 percent of successful cyberattacks begin with a phishing email.[v] In June 2023, *Forbes* released a report claiming that the United States experienced over 500 million phishing attacks in 2022, resulting in $52 million in losses.[vi] The same report also indicated that phishing attacks are on the rise, with the number of phishing attacks more than doubling between 2021 and 2022.

In response, CISA, NSA, FBI, and MS-ISAC—an organization focused on improving the cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organizations— have released updated, comprehensive guidance on addressing the threat. The new document goes beyond providing a 1–2-page high-level overview and details specific policies and technical configurations organizations can adopt to both prevent attacks and respond to them if they occur. Let's discuss their recommendations and explore how they may impact Health-ISAC members moving forward.

Beyond General Guidance and Recommendations

The guidance includes several specific mitigation strategies to address phishing for all organizations, as might be expected, but it also provides specific guidance to small- and medium-sized businesses (SMBs) and software manufacturers.
Recognizing that not all organizations have the personnel and resources to implement and sustain cutting-edge approaches to combatting phishing, the guidance dedicates a page-and-a-half to specific policies and controls for SMBs that includes recommendations to:

- Identify network phishing vulnerabilities, including by participating in CISA's Phishing Vulnerability Scanning Assessment Service.[vii]
- Implement DNS filtering or firewall denylists to block known malicious sites.
- Implement a secure virtual private network (VPN).
- Consider migrating to managed cloud-based email services with reputable third-party vendors.

Furthermore, the guidance aligns with recommendations from the national cyber strategy to reduce the burden of security on end users where possible. The guidance does this by advocating for software manufacturers to incorporate secure-by-design and secure-by-default into their development practices. According to the guidance, these measures should help "[reduce] the susceptibility [of software manufacturer] customers to phishing attacks."[viii]
More specifically, the guidance includes recommendations such as:

- Provide email products with internal mail and messaging monitoring mechanisms enabled by default.
- Consider implementing security notifications for the customer when non-secure configurations are used in email software products.
- Ensure phishing filtering and blocking mechanisms are packaged with email software by default to prevent successful malware deployment.

Beyond providing strategies to prevent phishing attacks, the guidance also details a six-step incident response model for organizations experiencing a phishing attack: 1) re-provision suspected or confirmed compromised user accounts; 2) audit account access; 3) isolating the affected workstation after the detection; 4) analyze the malware; 5) eradicate the malware; 6) restore systems to normal operations and confirm they are functioning properly.

CISA, NSA, FBI, and the MS-ISAC also encourage organizations to report phishing incidents directly to cloud email platforms (e.g., Microsoft Outlook), CISA, the FBI Internet Crime Complaint Center, or the MS-ISAC.

The recommendations are outlined in more depth within the Guidance for those interested.

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, October 31
No relevant meetings

Wednesday, November 1
No relevant meetings

Thursday, November 2
No relevant meetings

International Hearings/Meetings

-No relevant meetings

[i] https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf
[ii] https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-ncirp
[iii] https://www.cisa.gov/sites/default/files/2023-10/NCIRP-2024-Fact-Sheet-508C.pdf
[iv] https://www.cisa.gov/sites/default/files/2023-10/NCIRP-2024-Fact-Sheet-508C.pdf
[v] https://www.cisa.gov/shields-guidance-families
[vi] https://www.forbes.com/advisor/business/phishing-statistics/
[vii] https://www.cisa.gov/resources-tools/services/phishing-vulnerability-scanning#:%7E:text=Phishing%20vulnerability%20scanning%20sends%20a%20mock%20phishing%20email,the%20email%20to%20determine%20potential%20level%20of%20impa
[viii] https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf
[ix] https://www.hhs.gov/sites/default/files/multi-factor-authentication-smishing.pdf
[x] https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf
[xi] https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools
[xii] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Report Source(s)

Health-ISAC

Release Date

Oct 31, 2023, 11:59 PM

Reference | References

Health Industry Cybersecurity Practices
CISA
CISA
CISA
CISA
CISA
Health-ISAC
CISA
HHS
Forbes
CISA

Tags

Cybersecurity guidance, NCIRP, Hacking Healthcare, CISA, Phishing

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP "Share Threat Intel" Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.