July 6th, 2021

TLP White

This week, *Hacking Healthcare* begins by evaluating the National Institute of Standards and Technology's (NIST) definition of "critical software" and what that definition might mean for healthcare within the context of the cybersecurity executive order. Next, we take a look at a new US Cybersecurity & Infrastructure Security Agency (CISA) initiative for improving cybersecurity, and we assess whether focusing on bad practices is likely to make a noticeable difference. Lastly, we provide a brief update on how the Biden administration is considering tackling the scourge of ransomware, including some thoughts on offensive action, incident reporting, and the feasibility of banning of ransom payments. Welcome back to *Hacking Healthcare*.

1. **NIST Defines "Critical Software"**

   The Biden Administration's lengthy cybersecurity executive order is focused primarily on directly improving the federal government and federal contracting space. However, several sections within the executive order are expected to have impacts that go far beyond just those two areas. One such section, *Section 4. Enhancing Software Supply Chain Security*, may end up being particularly impactful for critical infrastructure sectors such as healthcare.

   Section 4 of the cybersecurity executive order notes that "the development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors."[1] In response to this, it highlights the need to "implement more rigorous and predictable mechanisms for ensuring that products function securely," with an emphasis placed on ensuring the security and integrity of "critical software."[2]

   However, "critical software" lacked a more formal definition until now. As part of section 4, NIST was tasked with defining just what qualifies as "critical software," and they recently published their work in a 10-page white paper entitled *Definition of Critical Software Under Executive Order (EO) 14028*.[3] Within that white paper, NIST provides the necessary background for this task, their approach, the definition, and explanatory material.[4]

In the white paper, NIST says that:
EO-critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

- Is designed to run with elevated privilege or manage privileges
- Has direct or privileged access to networking or computing resources
- Is designed to control access to data or operational technology
- Performs a function critical to trust; or,
- Operates outside of normal trust boundaries with privileged access

According to NIST, this definition "applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes."[5] Some of the broad categories NIST has initially determined fall under this definition include:[6]

- Identity, credential, and access management (ICAM)
- Operating systems, hypervisors, container environments
- Web browsers
- Endpoint security
- Network protection
- Backup/recovery and remote storage

This definition will now be used as the basis for guidance called for within the executive order.

Action & Analysis
Included with H-ISAC Membership

2. CISA to Focus On Bad Practices

From our "Hmmmm. Maybe?" department, we look at a June 24th blog post by CISA Executive Assistant Director Eric Goldstein where he announced the agency would take up a new initiative aimed at highlighting cybersecurity bad practices. If that sounds mildly counter to what CISA generally does, Goldstein helpfully elaborated on why he believes this approach to improving cybersecurity is necessary.

Acknowledging that CISA often focuses "on promoting best practices: the necessary steps that organizations must take to secure their enterprises," Goldstein believes it is just as important to highlight the kinds of bad practices that organizations should work towards ending.[7] He highlights in the blog post how "[t]here is certainly no lack of standards, practices, control catalogs, and guidelines available to improve an organization's cybersecurity," but that "the sheer breadth of recommendations can often be daunting for leaders and risk managers."[8]

In order to ensure that the massive amount of bad practices do not similarly overwhelm organizational leaders and risk managers, CISA is adopting the principle of "focus[ing] on

the critical few."[9] This approach will see CISA manage a small, targeted list of egregious risks and bad practices that organizations should tackle, and CISA hopes it will help organizations to prioritize efforts.

The list is applicable to all organizations, but NIST points out it may be especially useful for those designated as critical infrastructure or a National Critical Function (NCF). The current list includes just two items which are elaborated in more depth on CISA's website:

1. Use of unsupported (or end-of-life) software in service of Critical Infrastructure and National Critical Functions
2. Use of known/fixed/default passwords and credentials in service of Critical Infrastructure and National Critical Functions

Action & Analysis
Included with H-ISAC Membership

3. Ransomware Continues to Confound US Policy Responses

Ransomware's unceasing attacks, and the increasing tendency of malicious actors to victimize critical infrastructure, has greatly increased the danger ransomware poses. Unfortunately, it has largely confounded governmental guidance and policy solutions so far. The most recent reports coming from the Biden administration appear to suggest two new approaches are being considered in an effort to tamp down the threat.

Last Tuesday, it was reported that Deputy National Security Advisor Anne Neuberger supported the idea of pursuing offensive actions to disrupt ransomware groups and infrastructure.[10] She referenced earlier joint FBI, US Cyber Command, and private sector operations that went after botnet infrastructure as an illustration for how this kind of operation could work.[11] However, Neuberger also noted that such operations require more information and visibility to be effective.[12]

Part of creating a clearer picture may involve the government having a better sense of the scale of the issue. In trying to further understand that scale, as well as to potentially disincentivize ransomware payments, the Biden administration is allegedly looking at "whether to prohibit companies from keeping ransomware payments secret."[13] However, the Biden administration has not formally committed to that approach and has not outlined exactly what that could look like. One policy that appears likely to stay in place is the discouragement, but not outright banning, of ransomware payments generally. Neuberger stated that banning ransomware payment would be a "difficult policy position" to stand by[14], but that shouldn't be taken to mean that the administration won't pursue it in the future.

Action & Analysis
Included with H-ISAC Membership

July 6th, 2021

U.S. Congress –

Tuesday, July 6th:
- No relevant hearings

Wednesday, July 7th:
- No relevant hearings

Thursday, July 8th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

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

Contact us: follow @HealthISAC, and email at contact@h-isac.org

---

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[3] https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf

[4] https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf
[5] https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf
[6] https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf
[7] https://www.cisa.gov/blog/2021/06/24/bad-practices
[8] https://www.cisa.gov/blog/2021/06/24/bad-practices
[9] https://www.cisa.gov/blog/2021/06/24/bad-practices
[10] https://www.cyberscoop.com/biden-ransomware-cryptocurrency-neuberger/
[11] https://www.cyberscoop.com/biden-ransomware-cryptocurrency-neuberger/
[12] https://www.cyberscoop.com/biden-ransomware-cryptocurrency-neuberger/
[13] https://www.cyberscoop.com/biden-ransomware-cryptocurrency-neuberger/
[14] https://www.cyberscoop.com/biden-ransomware-cryptocurrency-neuberger/