Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 15d6a910 | Apr 20, 2023, 10:16 AM

This week, *Hacking Healthcare* examines new CISA guidance on secure-by-design/default, which received significant international support but left some in the private sector frustrated by the approach. Next, we break down three new, free cybersecurity resources published by the Department of Health and Human Services (HHS) that could help Health-ISAC members of all shapes and sizes.

Welcome back to *Hacking Healthcare*.

CISA Publishes Joint-International Notice on Secure-by-Design

On April 13, the Cybersecurity and Infrastructure Security Agency (CISA) published a joint guidance with a number of international partners on secure-by-design principles.[i] The general contents of the document may not surprise many, given that it touches on issues raised in the recent U.S. National Cybersecurity Strategy, but its choice of contributors and specific selections raises some questions around what industry should make of the document.

The publication, *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default*, is notable in the number of other government agencies from U.S.-allied countries that signed on to it. In addition to the usual U.S. government partners like the National Security Agency (NSA) and Federal Bureau of Investigation (FBI), Australia's Cyber Security Centre (ACSC), Canada's Centre for Cyber Security (CCCS), Germany's Federal Office for Information Security (BSI), the UK's National Cyber Security Centre (NCSC-UK), Netherlands' National Cyber Security Centre (NCSC-NL), and New Zealand's Computer Emergency Response Team (CERT NZ) and National Cyber Security Centre (NZ NCSC) all partnered on the report. One group notably absent from the process appears to be any stakeholders from the private sector.

The fifteen-page document opens by reiterating the Biden administration's call for those entities better positioned further up the supply chain to do more to help protect the customers and end users of products. The authoring agencies advocate for security to act as a "critical prerequisite to features and speed to market," with secure-by-design/default being core to the approach.[ii] Both secure-by-design and secure-by-default are detailed at length, but at a high level, the authoring agencies define these terms as:

Secure-by-Design: Products for which "the security of the customers is a core business goal, not just a technical feature."

Secure-by-Default: "Products are those that are secure to use 'out of the box' with little to no configuration changes necessary and security features [that are] available without additional cost."

Joint Recommendations

The body of the notice contains recommendations for software manufacturers on ways to approach software product security, secure-by-design tactics, secure-by-default tactics, and a few paragraphs aimed at customers/end users of such products. While we won't reproduce the entirety of the guidance here, the authoring agencies encourage technology manufacturers to adopt three core principles:

- The burden of security should not fall solely on the customer.
- Embrace radical transparency and accountability.
- Build organizational structure and leadership to achieve these goals.

The agencies go on to promote the use of the National Institute of Standards and Technology's (NIST) Secure Software Development Framework (SSDF), "a core set of high-level secure software development practices that can be integrated into each stage of the software development lifecycle (SDLC)."[iii] Alongside these SSDF items is an assortment of related call-outs to principles like defense-in-depth and nods to CISA's Cyber Performance Goals (CPGs). They then wrap up manufacturing recommendations with a half-dozen or so secure-by-default "tactics" that include encouraging the use of practices like single sign-on technologies and the removal of default passwords.

The final section, *Recommendations for Customers*, will look familiar to readers of Hacking Healthcare. The section implores organizations to "hold their supplying technology manufacturers accountable for the security outcomes of their products," and to prioritize acquiring technologies that follow secure-by-design/default principles. The section suggests putting policies in place that require security assessment prior to purchase and empowering IT departments to develop criteria and hold to them when encountering pushback.

Action & Analysis
Included With Health-ISAC Membership

HHS Publishes New Cybersecurity Resources

On April 17, the Department of Health and Human Services published three new online resources for the healthcare and public health (HPH) sector.[vi] These resources — consisting of a landscape analysis of hospital cyber resilience, a new educational platform, and the 2023 update to the Health Industry Cybersecurity Practices (HICP) — should be of great value to Health-ISAC members.

Knowledge on Demand[vii]

This new educational website describes itself as "a cybersecurity education platform that includes multiple delivery methodologies to reach the varied size health care facilities across the country."[viii] The site currently provides free training aimed at improving staff awareness and understanding of five of the top threats outlined in HICP:

- Social engineering
- Ransomware
- Loss or theft of equipment or data
- Accidental, intentional, or malicious data loss
- Attacks against network-connected medical devices

Trainings consist of a one-page overview, a PowerPoint presentation with notes, and a narrated educational video. The topics are addressed in an approachable, easy-to-understand manner that should appeal to a wide variety of non-experts on security while still providing some useful refreshers as background information for security teams.

Landscape Analysis[ix]

This 55-page report summarizes "domestic hospitals' current state of cybersecurity preparedness."[x] This paper is the product of HHS' and the Healthcare and Public Sector Coordinating Council's (HSCC) collaboration "to better understand the state of cybersecurity within U.S. hospitals" at a time when there is interest in formulating new laws and regulations to improve the sector's cybersecurity and resiliency. [xi] The body of the report consists primarily of sections on threat analysis, NIST Cybersecurity Framework and HICP coverage, and a breakdown of HICP practice adoption.

HICP 2023

The 2023 edition to HICP is a timely update to the HHS' and healthcare industry's joint guidance that was first published back in 2018. The new guidance has "been updated by over 150 industry and federal government professionals to include the most relevant and cost-effective ways to keep patients safe and mitigate the current cybersecurity threats that the HPH sector faces."[xii] New to this edition is a "discussion of the dangerous threat of social engineering attacks as one of the top five threats facing the sector."

Action & Analysis

Included With Health-ISAC Membership

Congress

Tuesday, April 18

No relevant hearings

Wednesday, April 19

No relevant meetings

Thursday, April 20

No relevant hearings

International Hearings/Meetings

No relevant meetings

[i] https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
[ii] https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
[iii] https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
[iv] https://insidecybersecurity.com/daily-news/goldstein-cisa-security-principles-software-intended-be-first-chapter-discussions-kick
[v] https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
[vi] https://www.hhs.gov/about/news/2023/04/17/hhs-cybersecurity-task-force-provides-new-resources-help-address-rising-threat-cyberattacks-health-public-health-sector.html
[vii] https://405d.hhs.gov/knowledgeondemand
[viii] https://405d.hhs.gov/knowledgeondemand
[ix] https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf
[x] https://www.hhs.gov/about/news/2023/04/17/hhs-cybersecurity-task-force-provides-new-resources-help-address-rising-threat-cyberattacks-health-public-health-sector.html
[xi] https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf
[xii] https://www.hhs.gov/about/news/2023/04/17/hhs-cybersecurity-task-force-provides-new-resources-help-address-rising-threat-cyberattacks-health-public-health-sector.html

---

Reference | References

CISA AA22-040A
Health-ISAC
HHS
HHS
HHS
insidecybersecurity

Report Source(s)

Health-ISAC

Tags

secure-by-design, Hacking Healthcare, Guidance, CISA, HHS

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare:

Written by John Banghart, who 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.

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

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.