Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 3885b642 | Apr 25, 2023, 02:28 PM

This week, *Hacking Healthcare* takes a look at two new cybersecurity proposals that could have major effects on cyber threat information-sharing across the European Union (EU), as well as on incident response and recovery for critical sectors like healthcare, and for healthcare entities that use managed security service providers.

Welcome back to *Hacking Healthcare*.

A New Proposed EU Cybersecurity Regulation

Last week, the European Commission published a proposal for regulation that will have significant impacts on EU-wide cybersecurity, should it be finalized. The Cyber Solidarity Act (CSA) has the potential to affect the healthcare sector positively across areas of security, resilience, information-sharing, and more, but it may also have some detrimental effects. Let's break them down and discuss how Health-ISAC members may wish to respond.

Cyber Solidarity Act

The scope of the CSA is rather ambitious. With the broad goal of "[strengthening] capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks," the proposal has three main objectives:[i]

- Strengthen common EU detection and situational awareness of cyber threats and incidents, and thus contribute to European technological sovereignty in the area of cybersecurity.

- Reinforce preparedness of critical entities across the EU and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making incident response support available [to entities] associated with the Digital Europe Programme (DEP).

- Enhance EU resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents, including drawing lessons learned and, where appropriate, recommendations.

To achieve these objectives, the proposal further details the following actions:[ii]

- The deployment of a European Cyber Shield, a pan-European infrastructure of Security Operations Centres (SOCs), to build and enhance common detection and situational awareness capabilities.

- The creation of a Cyber Emergency Mechanism to support member states in preparation for, response to, and immediate recovery from significant and large-scale cybersecurity incidents. Support for incident response shall also be made available to European institutions, bodies, offices, and agencies of the European Union (EUIBAs).

- The establishment of a European Cybersecurity Incident Review Mechanism to review and assess specific significant or large-scale incidents.

Funding for these initiatives will come in part from Digital Europe Programme. The proposal is currently open for an eight-week feedback period that will help to inform discussions between the European Parliament and the European Council.

Action & Analysis
Included with Health-ISAC Membership

Cybersecurity Act Amendment for Managed Security Services

In addition to the Cyber Solidarity Act, the European Commission also published a proposal to amend the Cybersecurity Act. The amendment would introduce cybersecurity certification schemes for managed security services. For those healthcare entities that rely on managed security services, this amendment is likely to be beneficial but could raise some costs.
To level set, the proposal notes that managed security services play important roles covering the aspects of prevention, detection, response, and recovery. They are described as providing "services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management" and operate in such areas as "incident response, penetration testing, security audits and consultancy."[x]

With managed security services playing "an increasingly important role in the prevention and mitigation of cybersecurity incidents" and given past commitments by EU member states to "raise the overall level of cybersecurity," a certification scheme would appear to track with the goal of "[encouraging] the emergence of a trusted cybersecurity service industry."[xi] The proposed amendment also appears to want to head off the possibility of EU states creating their own unaligned certifications for managed security services.

Action & Analysis
Included with Health-ISAC Membership

Congress

Tuesday, April 25

No relevant hearings

Wednesday, April 26

No relevant meetings

Thursday, April 27

No relevant hearings

International Hearings/Meetings

No relevant meetings

[i] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[ii] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[iii] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[iv] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[v] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[vi] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[vii] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[viii] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[ix] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13816-Cyber-Solidarity-Act_en

[x] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13815-The-Cyber-Skills-Proposal-Amendment_en

[xi] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13815-The-Cyber-Skills-Proposal-Amendment_en

[xii] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13815-The-Cyber-Skills-Proposal-Amendment_en

---

Reference | References

Europa Analytics
Health-ISAC
Europa Analytics

Report Source(s)

Health-ISAC

Tags

Cyber Solidarity Act, Regulation, Hacking Healthcare, EU, Information Sharing

---

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:

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.