



Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare

TLP:WHITE

Alert ID : 3b098b99

Sep 08, 2023, 01:55 PM

This week, *Hacking Healthcare*TM catches up with the revision to the European Union's Network and Information Security (NIS) Directive, NIS2. We review what NIS2 is, how Health-ISAC members may be affected, where NIS2 is in its implementation timeline, and what actions Health-ISAC members may wish to consider taking at this time.

Welcome back to *Hacking Healthcare*TM.

The Health-ISAC Hobby Exercise 2023

Before we get to NIS2, the Health-ISAC is pleased to announce the 4th iteration of our Hobby Exercise on October 25th in Washington DC. The Hobby Exercise is an annual Healthcare and Public Health (HPH) event designed to engage the healthcare sector and strategic partners on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for organizational continuous improvement while increasing healthcare sector resiliency.

Members wishing to know more or express an interest in participating should visit the following registration link: <https://portal.h-isac.org/s/community-event?id=a1Y7V00000VJ560UAD>

NIS 2 Implementation Update

Health-ISAC will be holding several NIS2 sessions and discussions at the upcoming European Union (EU) Summit in Dubrovnik, Croatia. If you're interested in attending, please click [here](#) for more information on how to register.

It's been a while since we checked up on the revision to the European Union's Network and Information Security (NIS) Directive, and we thought it might be a good to review how NIS2 stands to impact the healthcare sector, where along the implementation path NIS2 is for the various EU member states, and what healthcare entities may wish to consider doing at this stage to prepare for it.

Let's start with a quick recap of what NIS2 is. The original NIS was the "first piece of EU-wide cybersecurity legislation" and was designed to improve cybersecurity across the EU, however, it fell a bit short on scope and its implementation was uneven and inconsistent across member states.^[i] NIS2 is

more stringent in its implementation and more comprehensive in who it applies to and what it seeks to address. For the healthcare sector, NIS2 will:

- Include broader and more consistent coverage of healthcare entities across EU member-states;
- Strengthen and harmonize cybersecurity requirements, including “Management Body” oversight and accountability;
- Streamline incident-reporting obligations to minimize over-reporting and the burden placed on private sector entities, and;
- Improve information-sharing, cooperation, and cross-border crisis management of cyber incidents.

NIS2 also complements the larger EU digital/cyber strategy elements found in the Cyber Resilience Act (CRA), the Digital Services Act (DSA), the Digital Markets Act (DMA), and others. EU member states were given until October 17, 2024, to successfully transpose the measures outlined in the NIS2 text into their own national laws, and member states were instructed to begin applying those measures as of October 18, 2024.

So where are we currently in the transposition process and what might Health-ISAC members consider doing at this time?

Action & Analysis

****Available with Health-ISAC Membership****

Congress

Tuesday, September 5th

No relevant hearings

Wednesday, September 6th

No relevant meetings

Thursday, September 7th

No relevant meetings

International Hearings/Meetings

No relevant meetings

EU

[i] <https://www.enisa.europa.eu/topics/nis-directive>

[ii] <https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs>

[iii] <https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs>

[iv] <https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs>

[v] <https://eur-lex.europa.eu/eli/dir/2022/2555>

Report Source(s)

Health-ISAC

Reference | References

[Health-ISAC](#)

[Europa Analytics](#)

[Europa Analytics](#)

[Europa Analytics](#)

[Health-ISAC](#)

Tags

NIS2, Hobby Exercise, Hacking Healthcare, European Union (EU)

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.