Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare **TLP:WHITE** **Alert Id: 5541e619** **2022-12-01 13:23:55**

This week, Hacking Healthcare begins by examining Australia's recent decision to deploy further active, offensive cyber measures through its new cyber task force. We attempt to understand how this may catalyze other governments to embrace a more offensive approach to cyber threats. Next, we catch you up on developments with the update to the EU's Network Information Security (NIS) Directive, including when entities should expect to it to enter into force.

Welcome Back to *Hacking Healthcare.*

Australia to "Hack Back" with Enhanced Offensive Cyber Operations

The Australian government formalized a new partnership between the Australian Federal Police (AFP) and Australian Signals Directorate (ASD) to investigate, target, and disrupt cybercriminal syndicates via information-sharing, collaboration, and enforcement activities.[i] The task force comes in response to recent data breaches against Optus and Medibank, and it signals a growing sense of urgency among governments to actively counter cybercriminal activity.

For those unfamiliar with the two Australian agencies in the task force, ASD's equivalent in the United States is the National Security Agency (NSA) and AFP's equivalent is the Federal Bureau of Investigation (FBI). Although the details of what issues this joint operation will focus on are ambiguous — and they may stay that way to prevent active cyber operations from being compromised —

generally, it can be expected that it will focus on intelligence gathering and threat hunting, specifically regarding ransomware threats. According to the Australian Cyber Security Centre's 2022 Cyber Threat Report, "ransomware remains the most destructive cybercrime threat to Australia due to its high financial impact and its targeted data breaches."[ii] Just in the last two months alone, Australia suffered serious hacks against Optus, its second-largest telecommunications company, and Medibank, its largest private health insurer. Between the two, "over 14 million customer accounts have had data hacked — equivalent to 56% of the population — since Sept. 22 alone."[iii]

Action & Analysis

Included with Health-ISAC Membership

NIS 2 Heads Toward Implementation

The European Union's Network and Information Security (NIS) Directive was the first EU- wide piece of legislation that set baseline cybersecurity expectations and requirements for EU member-states. As technology and cyber threats have evolved, the EU has been diligently working on a comprehensive update that has cleared its last procedural hurdles. The new NIS directive, NIS2, will bring about significant impacts on healthcare sector cybersecurity.

For those who haven't thought about NIS2 recently, or who need help remembering the difference between NIS2, the Cyber Resilience Act (CRA), and other EU legislation, let's quickly recap some of the significant ways that NIS2 will impact the healthcare sector:

- Broader and more consistent coverage of healthcare entities across EU member-states
- Strengthened and harmonized cybersecurity requirements that include "Management Body" oversight and accountability
- Streamlined incident-reporting obligations to minimize over-reporting and the burden placed on private sector entities
- Improved information-sharing, cooperation, and cross-border crisis management

When Will NIS2 Be Implemented?

While the final text was agreed upon between the European Parliament and the European Council back in May, it still needed to be formally adopted by both bodies. Parliament adopted it on November 11th, and the Council did the same on November 28th. All that is left is for NIS2 to be published in the Official Journal of the European Union, which appears likely to happen in the next few days.

Twenty days after its publication in the journal, NIS2 will enter into force and the clock will start for EU member-states to transpose the provisions of the directive into their own national law. Member-states will have 21 months to complete this task, and while there is certain to be staggered completion among the various members, NIS2 will become uniformly enforced after the 21-month deadline.

Action & Analysis

Included with Health-ISAC Membership

Congress

Tuesday, November 29th:

- No relevant hearings

Wednesday, November 30th:

- No relevant hearings

Thursday, December 1st:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

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

[i] https://www.theepochtimes.com/hacking-back-australia-launches-hunt-for-cyber-syndicates_4860888.html?welcomeuser=1

[ii] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022#Ransomware

[iii] https://www.reuters.com/technology/australia-hacking-frenzy-spurred-by-an-undersized-cybersecurity-workforce-2022-10-31/

[iv] Five Eyes Alliance: United States, United Kingdom, Canada, Australia, New Zealand

[v] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0383_EN.pdf

Reference(s): theepochtimes, Australian Government, Europa Analytics, Reuters, Australian Government

Report Source(s): Health-ISAC

Tags: NIS2, Hacking Healthcare, Ransomware

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.