May 3, 2022

TLP White

This week, Hacking Healthcare examines a new report from the European Union Agency for Cybersecurity (ENISA) on the state of coordinated vulnerability disclosure (CVD) within the EU. In addition to outlining the challenges to CVD policy alignment we discuss the Health-ISACs role in the CVD process. Next, we explore what appears to be coordinated sabotage of internet infrastructure in France and reiterate the importance of planning for unforeseen service outages. Finally, we cover a concerning new cybersecurity incident reporting regime coming into force in India.

Welcome back to *Hacking Healthcare*.

1. **Coordinated Vulnerability Disclosure In the EU**

   For those not as familiar with the term, CVD can generally be described as the process by which those that find software or hardware vulnerabilities communicate those vulnerabilities to the various relevant stakeholders (e.g. vendors, ISACs, government agencies, etc.…) and by which those stakeholders then disclose those vulnerabilities and their mitigations publicly. National CVD policies are often designed to explain under what circumstances researchers may be authorized to probe for vulnerabilities within products, how vulnerabilities should be communicated once found, who should receive them (e.g. vendors or government agencies), and what length of time vendors or developers should be given to mitigate vulnerabilities prior to public disclosure. These policies are intended to incentivize the responsible disclosure of vulnerabilities in a way that balances the competing objectives of the various stakeholders involved for the betterment of cybersecurity as a whole.

   Published on April 13th, ENISA's *Coordinated Vulnerability Disclosure Policies In The EU* is a hefty 90-page document that usefully outlines the state of CVD within each of the EU's member states in addition to a few select regions like China and the United States. Beyond illustrating the "substantial differences" that exist between the various national

level policies, the report also highlights just how many countries have yet to even begin considering how to establish a national CVD policy.

According to ENISA, only four member states have a fully established national CVD policy. Another four member states are "on the point of implementing a policy" by either examining a proposal or piloting one.[1] A further ten member states are "in the process of implementing a national CVD policy or are on the point of doing so," but have failed to reach a political or legislative consensus on the process. Finally, nine member states have not even begun the process for establishing one.[2] Although it is worth noting that while some countries lack a formal CVD process, in some cases "current practices or legal frameworks in place in the countries already allow CVD processes to take place."[3]

Accompanying the summary of the CVD in the EU member states is a breakdown of how ENISA views CVD policy. This includes an examination of desired elements in a CVD process, good practices, and known challenges and issues.

Action & Analysis
Membership required

2. Suspected Sabotage of French Fiber Optic Cables

On Wednesday of last week, a spate of attacks against fiber optic cable infrastructure in France disrupted internet service for tens of thousands of individuals. What appears to be a coordinated act of sabotage has highlighted the difficulty in protecting internet infrastructure and reiterated a risk that critical infrastructure entities must be prepared for.

Internet service disruptions were reported in several major French cities as multiple fiber optic cable lines appear to have been purposefully targeted and cut for as of yet unknown reasons. Internet service providers FREE and SFR each reported service outages that required significant time to repair as "key" backbone cables were targeted.[4] Despite the attacks going far beyond the occasional construction accident or animal related damage, FREE reported that a relatively small number of its users (~40,000) were ultimately impacted, and it was reported that no hospitals were affected.[5, 6]

The attacks have been called unprecedented and extraordinary by cybersecurity experts like Ciaran Martin, formerly the CEO of the UK's National Cyber Security Centre (NCSC), and Bob Kolasky, the former director of the Cybersecurity and Infrastructure Security

Agency's (CISA) National Risk Management Center (NRCM).[7] Since the attack, French authorities from the cyber section of the Paris Public Prosecutor's office have reportedly begun investigating the incident as a criminal matter and they have been joined by the General Directorate for Internal Security (DGSI), a French "special intelligence service under the authority of the Ministry of Interior."[8, 9]

Action & Analysis
Membership required

3. India Takes Cybersecurity Incident Reporting to the Extreme

Cybersecurity incident reporting has become a hot topic worldwide over the past few years. While sector specific and state level reporting regimes have existed for some time, governments and their legislatures are increasingly entering into the space with hopes of improving visibility into the state of their digital ecosystem. Differences abound between these various newly constructed or considered regimes, but India's newly announced policy has gone further than most.

On April 28th, the Indian Computer Emergency Response Team (CERT-In) issued a notice about "directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet."[10] Citing "gaps causing hindrance in incident analysis," CERT-In's directions under the provisions of sub-section (6) of section 70B of the Information Technology Act, 2000 could have drastic implications for affected organizations.[11]

Some of the new direction's requirements include:[12, 13]

- Service providers, intermediaries, data centers, body corporate and Government organizations must report cybersecurity incidents to CERT-In within 6 hours of noticing them or having them reported to them by a third party
- An expansive list of mandated reporting incidents that includes scanning/probing of critical networks/systems, defacement of websites, spoofing and phishing attacks, and Distributed Denial of Service (DDoS)
- Guidelines for VPS (virtual private server), Cloud Service providers, and VPN (virtual private network) service providers that will require data retention of users for up to five years

The notice was published on April 28th and will enter into force 60 days hence.

Action & Analysis
Membership required

May 3, 2022

Congress

Tuesday, May 3rd:
- No relevant hearings

Wednesday, May 4th:
- No relevant hearings

Thursday, May 5th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Conferences, Webinars, and Summits

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

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

About the Author

Hacking Healthcare is 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, and 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.

---

[1] https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

[2] https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

[3] https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

---

[4] https://www.datacenterdynamics.com/en/news/multiple-fibers-cut-across-france-impacting-several-cities/

[5] https://www.bloomberg.com/news/articles/2022-04-27/attacks-on-french-fiber-networks-causes-internet-outages

[6] https://www.rfi.fr/en/science-and-technology/20220428-france-investigates-suspected-sabotage-of-fiber-optic-cables-that-disrupted-internet

[7] https://www.cyberscoop.com/french-fiber-optic-cables-attack-critical-infrastructure/

[8] https://www.bloomberg.com/news/articles/2022-04-27/attacks-on-french-fiber-networks-causes-internet-outages

[9] https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/our-missions

[10] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1820904

[11] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1820904

[12] https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[13] https://www.bleepingcomputer.com/news/security/india-to-require-cybersecurity-incident-reporting-within-six-hours/