Hot doc: Cyber Resilience Act sticking points

POLITICO Pro Cyber Insights Europe <cyberinsights@politico.eu> 6 November 2023 at 15:56

Pro Cyber Insights

By ANTOANETA ROUSSI

with JOSEPH GEDEON

PRESENTED BY

Instagram

View in your browser or listen to audio

TODAY'S TOP LINE — POLITICAL HICCUPS: Lawmakers continue to negotiate on the Cyber Resilience Act this week, but contentious areas like vulnerability reporting and open-source software are nowhere near done. We have the docs to show it.

Welcome to Cyber Insights, POLITICO's cybersecurity and data protection newsletter, giving you the daily lowdown on hacks, leaks and cybersecurity policy chatter in Europe.

How to reach us: Antoaneta is at @antoanetaroussi and aroussi@politico.eu. Clothilde is at @clothildegouj and cgoujard@politico.eu. Laurens is at @laurenscerulus, lcerulus@politico.eu and Signal and WhatsApp at +32498606816

CYBER RESILIENCE ACT

HOT DOC — CRA FOUR-COLUMN: The finish line is in sight for the European Union's Cyber Resilience Act, the law that's meant to better secure internet-connected devices across the bloc.

But there are still significant hurdles to overcome, judging from a leaked copy of the four-column document showing compromises between the European Commission, the European Parliament and the Council of the EU's proposals and obtained by Cyber Insights. See it here first.

— Article 11 is still the most contentious i.e. to whom manufacturers of digital products should **report unpatched vulnerabilities**. In the compromise text, it's clear that the negotiators haven't been able to reach an agreement on who will handle a database with glitches: the EU's cybersecurity agency ENISA or or national Computer Security Incident Response Teams (CSIRT). This issue will now be handed over to the political level.

— Also on vulnerabilities, Parliament proposed that where a notified vulnerability "has no corrective or mitigating measures available" ENISA shall ensure that information is shared in line with strict security protocols and on a **need-to-know** basis. That proposal will be integrated in a Commission compromise on the article.

— On **open-source**, another sticking point, it seems there's been no consensus either. The Commission drafted proposed compromise language that says "*only* free and open-source software *made available on the market,* and therefore supplied for distribution or use, in the course of a commercial activity should be covered by this Regulation. *Whether a free and open-source* software *product has been made available as part of a commercial activity should be assessed on a* case-by-case *basis,*" according to the draft compromise seen by Cyber Insights. (We kept the italics to emphasize the changes.)

This seems a concession to open-source organisations like the Linux Foundations, who have lamented the risks that the cyber law could cripple the open-source not-for-profit model that underpins many of the internet's protocols and

mechanics. But let it be clear: This wording is far from greenlit by political negotiators.

— A new recital proposed by Parliament also poses that products with digital elements that are developed "exclusively for **national security or military purposes**" or to handle classified information will not be captured by the regulation. Nevertheless, countries are encouraged to ensure the same or higher level of protection for those products.

Timing: Political negotiations on the bill are set to continue Wednesday (November 9) and another round is scheduled for November 30. Negotiators want to land a deal before the end of the year but judging from the mood among those involved, it could even be the end of this month.

ENCRYPTION

OMBUDSMAN WEIGHS IN ON CHILD SEXUAL ABUSE LAW: The European Ombudsman has found the European Commission conducted maladministration when it failed to disclose a list of experts consulted on the technical feasibility of detecting CSAM without undermining encryption.

A wide group of privacy advocates and academics have warned repeatedly that it is not possible to detect child sexual abuse material (CSAM) at the scale proposed by the Commission without breaking encryption entirely. But the Commission relied on a group of experts that professed it can be done.

When asked by The Irish Council for Civil Liberties to disclose the names of the experts consulted in drafting the text related to potential solutions to detect child sexual abuse material in end-to-end encrypted communications, the Commission refused.

"The Ombudsman found that the Commission had indeed failed to identify a document, namely a list of experts that clearly fell within the scope of the complainant's requests," a statement by the Ombudsman reads. "The Ombudsman considered that this constitutes maladministration."

In line with its finding, the Ombudsman suggests that the Commission give public access to the list of experts.

Previously, the chair of the lead civil liberties committee asked Home Affairs Commissioner Ylva Johansson for explanations regarding alleged conflicts of interest on the law on child sexual abuse material. Lawmaker Juan Fernando López Aguilar (Social Democrat, Spain) said reports published in different media outlets about close connections between the Commission and some children's and tech groups could indicate "possible undue influence in the drafting of the proposal."

ICYMI: On Friday, the Ombudsman office also announced it had started an inquiry into the European Data Protection Supervisor's (EDPS) failure to publish documents concerning its use of social media and published a decision on the EDPS refusal to publish preparatory documents for its guidelines on international data transfers.

COURTS

SKY ECC TRIAL POSTPONED: Well, that's a bummer. We built the excitement on Friday that Belgium was kicking off its behemoth criminal trial hinging on data acquired in the Sky ECC and EncroChat encryption busts by Belgian, French and other European police. Investigators look to jail and punish more than 120 defendants for crimes ranging from drug and arms trafficking to attempted murder and acts of torture.

But the case has been pushed back after attempts by defense attorneys to disqualify judges involved in the case, local media reported just after this newsletter hit your inboxes Friday.

(Re-)mark your calendar: The procedure is now postponed by four to six weeks, approximately, as the Court of Appeals considers the requests to oust judges, one of the defense lawyers involved told POLITICO's Elisa Braün.

CYBER CONFLICT

GAZA BLACKOUT: A third telecommunications blackout in 10 days again plunged Gaza into total darkness on Sunday — but this time it comes as United States Secretary of State Antony Blinken traverses the region pushing for a humanitarian pause in fighting in the blockaded Strip.

The "new collapse in connectivity" across Gaza, first reported by global internet monitoring group Netblocks, knocked out Gaza's last major telecoms provider to provide connectivity: Paltel.

"The disruption happens pretty much exactly at the moment the large airstrikes hit Gaza in livestreams," Netblocks founder Alp Toker told POLITICO's U.S. cyber colleagues. "And that would point to kinetic impact rather than a premeditated blackout."

Still, a previous airstrike that knocked out network connectivity in Gaza for over a day last month was met soon after with a widely-anticipated ground invasion — perhaps a signal that another significant operation is coming while the internet is down this latest time. The first outage lasted around 36 hours, while the second outage lasted a few hours. The connectivity was still out as of Sunday night.

THREAT REPORT

CYBER BATTLE: Hackers linked to the Iranian government spent much of 2023 targeting the Israeli education and technology sectors even before the October 7 attacks by Hamas on Israel, research published Monday finds.

A report from cybersecurity group Palo Alto's Unit 42 found that a group known as "Agonizing Serpens" aimed cyberattacks against these Israeli organizations between January and October of this year. Unit 42 researchers have tracked Agonizing Serpens since 2020, and assessed that it has "strong links" to Iran.

The attacks have involved data theft and the use of wipers to try to destroy the systems targeted and erase their tracks. The threat group then publishes this data on social media or Telegram, and Unit 42 researchers concluded that the likely goal is to "sow fear or inflict reputational damage," along with "inflicting considerable damage by wiping as many endpoints as possible."

Wider context: The research was compiled during dates prior to the Hamas attacks on Israel early last month. Hamas is known to be backed by the Iranian government, which has launched cyberattacks against Israel often in the past — with Israel having also launched high-octane attacks against Iran as well.

AGENDA

MILITARY 5G: If you're interested in how 5G tech is making its way into military tech, the Atlantic Council holds a discussion on it later today for a D.C. audience.

ELSEWHERE ON THE WEB

Microsoft vows to revamp security products after repeated hacks. Bloomberg

Cyber Insights wouldn't happen without Laurens Cerulus, Aoife White and Kelsey Hayes.

Pro Intelligence Connections

2022/0272(COD) Cyber Resilience Act
Committee decision to enter into interinstitutiona…