SECTRA NEWSLETTER – APRIL 2025

Monthly Review

Cybersecurity news from around the world

ARTICLE

Geopolitical impact: The fragility of cybersecurity

Read article →

SECTRA

General cybersecurity news

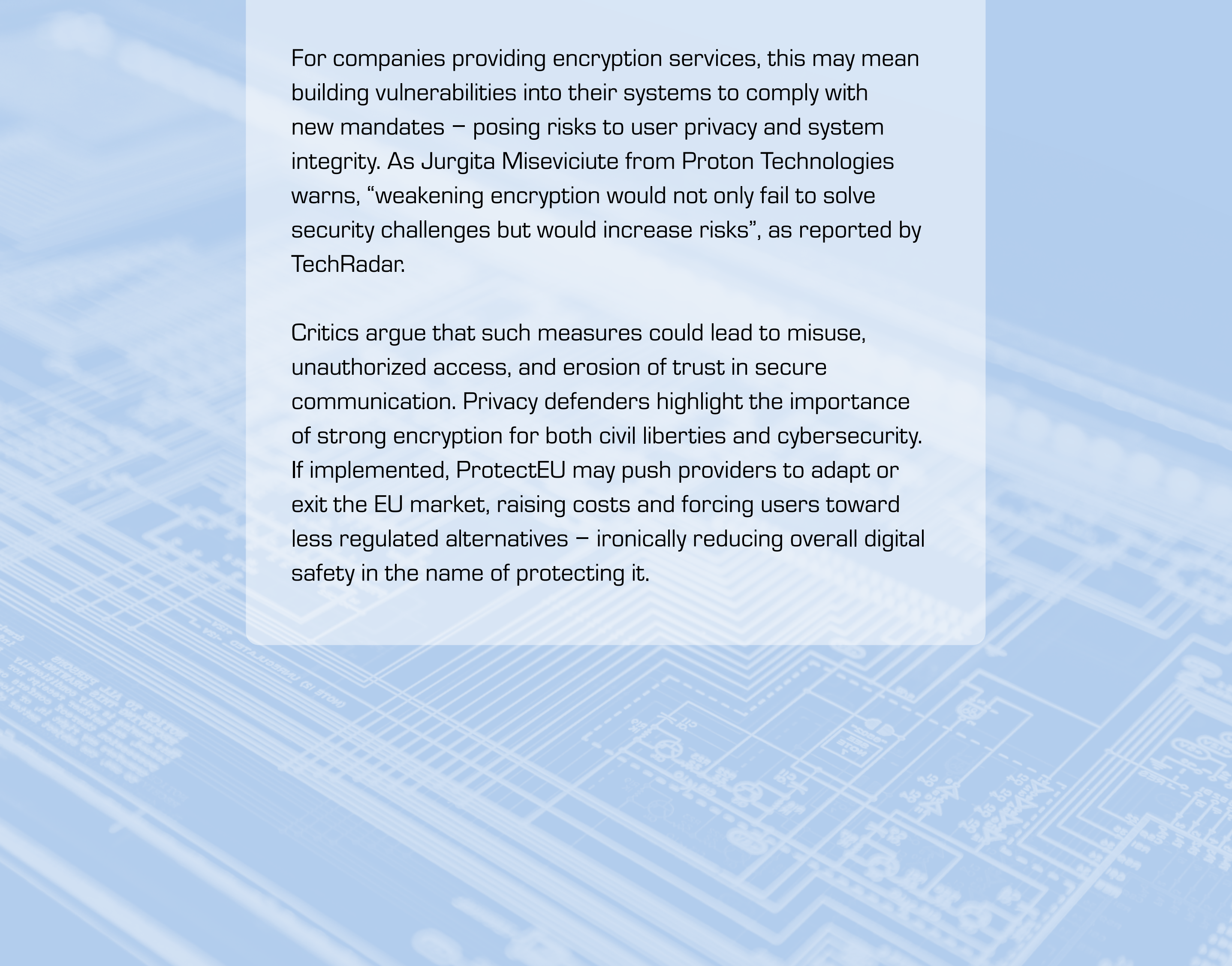
1

EU’s ProtectEU-plan sparks encryption concerns

The EU Commission introduced the ProtectEU strategy in early April. It aims to strengthen internal security by granting law enforcement legal access to encrypted data, a step described as crucial for tackling serious threats, according to the European Commission. While seeking to balance security and fundamental rights, the strategy includes encryption backdoors, which could weaken digital protections for users.

For companies providing encryption services, this may mean building vulnerabilities into their systems to comply with new mandates – posing risks to user privacy and system integrity. As Jurgita Miseviciute from Proton Technologies warns, “weakening encryption would not only fail to solve security challenges but would increase risks”, as reported by TechRadar.

Critics argue that such measures could lead to misuse, unauthorized access, and erosion of trust in secure communication. Privacy defenders highlight the importance of strong encryption for both civil liberties and cybersecurity. If implemented, ProtectEU may push providers to adapt or exit the EU market, raising costs and forcing users toward less regulated alternatives – ironically reducing overall digital safety in the name of protecting it.



2 Millions of Swede’s information leaked – after massive breach

Data breaches are increasing annually, often exposing highly sensitive information such as personal details, health records, political affiliations, and financial data. These incidents place individuals at significant risk of fraud, identity theft, and scams. If your data is compromised in a cyberattack, act immediately: Change passwords, enable two-factor authentication, monitor bank accounts, and be cautious about phishing attempts. Notify your bank or insurance provider, consider a credit freeze or identity protection service, and report the incident to authorities or cybersecurity agencies.

The urgency of preparedness was highlighted in January when a cyberattack on the Swedish sports platform SportsAdmin suffered a cyberattack exposing the data of two million Swedes across more than 1,700 sports clubs – making this one of the most severe data leaks in Swedish history.

3 EU announces plans to boost cybersecurity capabilities

The European Cybersecurity Competence Centre (ECCC) has adopted its Digital Europe Work Program 2025-2027, allocating €390 million to strengthen EU cyber resilience. The plan includes investments in advanced technologies, like AI and post-quantum transition, improved threat detection tools, and support for small and medium-sized enterprises (SMEs) to meet cybersecurity standards.

This decision comes as cyber threats grow and critical infrastructure faces increasing risks. It aims to address vulnerabilities, improve coordination across Europe, and align with key regulations such as NIS2, GDPR, and the Cyber Resilience Act.

The program will fund the development of scalable AI systems, secure products, and post-quantum infrastructure, benefiting industries, SMEs, and critical sectors like healthcare and communication networks. It also supports the implementation of the Cyber Solidarity Act, including a pan-European alert system and Cyber Hubs for coordinated detection.

ARTICLE

NIS2 in focus – Finland leads the way

As the EU's NIS2 Directive reshapes national cybersecurity standards, Finland has taken the lead with its new legislation already in force. Meanwhile, Sweden is catching up, creating a dynamic landscape for Nordic organizations navigating new compliance requirements.

Both Finland and Sweden are taking important steps to strengthen their national cybersecurity and align with the EU's NIS2 Directive. Yet, while Finland's new cybersecurity legislation has already come into force as Sweden's legislative response is still underway – highlighting varying levels of regulatory readiness across the Nordics.

On April 8th, Finland's Parliament passed the Cybersecurity Act to implement NIS2. The new legislation broadens the scope of cybersecurity obligations, now covering sectors such as public administration, food production, and waste management. It introduces stricter requirements for risk management, incident reporting, and documentation. Additionally, supervision will be decentralized to sector-specific authorities, and non-compliance will result in sanctions.

Meanwhile, Sweden has also strengthened its cybersecurity posture through their new National Cybersecurity Strategy for 2025–2029, presented by Carl-Oskar Bohlin, Sweden's Minister for Civil Defense, in March 2025. The Swedish strategy outlined priorities for systematic cybersecurity efforts, competence development, and enhanced ability to prevent, detect, and manage cyber incidents. →

However, Sweden's legislative response to NIS2 is still under preparation. According to MSB, the Swedish Civil Contingencies Agency, a new legislation, similar to the one in Finland, may come into effect as early as the summer of 2025.

Both countries are showing strong commitment to enhancing national cybersecurity and meeting EU requirements. However, there is a notable difference in timelines: Finland's Cybersecurity Act is already set in to action, while it will take some time before Sweden's is finalized and accepted. As for now, Finland's approach, with decentralized oversight and the introduction of clear sanctions, reflects a more immediate and structured implementation of NIS2.

> *"Finland's early legislative action sets a benchmark for swift compliance, while Sweden's broader strategy underlines the importance of long-term capacity building"*

For organizations navigating this new regulatory landscape, establishing continuous cybersecurity monitoring and incident response capabilities will be crucial. Investments in Security Operations Centers (SOC) and Managed Detection and Response (MDR) services can provide organizations with real-time threat detection, risk management, and compliance support.

A SOC is a dedicated team that continuously monitors an organization's network, looking for signs of cyberattacks, breaches, or vulnerabilities. It offers real-time analysis of security incidents and facilitates immediate responses. MDR services, combine technology and human expertise to detect and respond to advanced threats. →

These services offer a practical and scalable way to meet requirements for continuous monitoring, early incident detection, and efficient response – key elements emphasized both in the Finnish Cybersecurity Act and the Swedish national strategy.

As cyber threats continue to evolve and regulatory demands tighten, resilience will increasingly depend on proactive, structured security practices. Finland's early legislative action sets a benchmark for swift compliance, while Sweden's broader strategy underlines the importance of long-term capacity building.

Closing the gap between policy and operational cybersecurity will be critical. Organizations that invest early in continuous monitoring and incident response capabilities – such as SOC and MDR services – will be better positioned to meet both today's and tomorrow's cybersecurity challenges.

To align with NIS2, your organization should begin by reviewing the specific requirements for your sector. Reach out to your national cybersecurity authority or consult with experts to understand what needs to be implemented. Taking these steps, combined with implementing services like SOC and MDR, will significantly help your organization proactively prevent and mitigate the risk of cyberattacks. ■

ARTICLE

Geopolitical impact: The fragility of cybersecurity

MITRE’s CVE program, a cornerstone of global cybersecurity, faces uncertain times after the U.S. government ended its funding. On the same day, CISA stepped in and what does this mean for our digital security?

On April 16, 2025, the U.S government, announced that MITRE, the organization responsible for the CVE (Common Vulnerabilities and Exposures) program, would end its funding for the project. This unexpected decision caused concern in the cybersecurity world, especially among those who rely on CVE’s database to identify and manage software vulnerabilities. However, the same day, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) stepped in, announcing that CVE funding would continue. This support brought relief to those reliant on CVE’s functions to secure IT systems globally.

CVE, established in 1999, serves as a database for security flaws, allowing organizations and cybersecurity experts to share critical vulnerability information. It has become a vital component of global efforts to maintain security by providing a common framework to identify vulnerabilities, which enables quicker fixes and risk reduction. Organizations can implement patches and security updates in a more coordinated manner, preventing attackers from exploiting known flaws. →

Without the CVE system, businesses and governments would lack a unified standard for understanding and addressing threats. For example, without CVE's reference system, different organizations might struggle to coordinate their identification of vulnerabilities, leading to inefficiencies in collaboration and delays in cybersecurity responses.

Despite the initial alarm over MITRE's announcement, CISA's intervention provided reassurance by ensuring continued funding. However, the event raised questions about the system's long-term stability. While CISA's involvement calmed immediate fears, it also cast a spotlight on the issue of digital sovereignty – particularly for European countries concerned about their reliance on an American institution like MITRE.

> *"CVE is the heart of the cybersecurity ecosystem. Without it, we'd struggle to protect systems from widely known vulnerabilities"*

Reactions to MITRE's initial decision highlighted the system's importance. Cybersecurity experts warned that losing CVE would create an information vacuum, severely disrupting international security efforts. "CVE is the heart of the cybersecurity ecosystem," noted one expert. "Without it, we'd struggle to protect systems from widely known vulnerabilities."

While CVE's future now appears stable with CISA's support, digital sovereignty remains a pressing concern, particularly for EU nations. ENISA, the European Union Agency for Cybersecurity, has been vocal about the need to strengthen European-made solutions for vulnerability management. →

Reliance on external actors like MITRE and CISA complicates efforts to build independent, self-sufficient systems to address vulnerabilities. The uncertainty introduced by MITRE's initial move underscores a broader challenge for global cybersecurity – should more states and regions take greater control of their own security databases to ensure independence? For the EU, the situation may accelerate efforts to develop alternative systems and reduce reliance on external organizations.

ENISA's initiatives represent an early step in this direction, but more comprehensive efforts may follow. CVE's funding crisis revealed the fragility of global cybersecurity systems, emphasizing the importance of long-term planning. CISA's intervention addressed the immediate issue, but the event underscored the interconnectedness of cybersecurity efforts. Digital sovereignty remains critical, especially in Europe, as nations balance collaboration and independence. For organizations, the crisis is a stark reminder of cybersecurity's evolving nature, where complacency is not an option. ■

Key takeaways

1. ProtectEU's encryption access raises privacy and trust concerns in secure communication.

2. Data breaches are escalating, exposing sensitive information and increasing risks of fraud, identity theft, and scams.

3. The ECCC's €390M program boosts EU cyber resilience through AI, post-quantum security, and SME support.

4. Finland and Sweden demonstrate strong commitment to enhancing cybersecurity and aligning with NIS2 directives.

5. CISA's backing of CVE ensures stability but raises EU concerns about cybersecurity independence.

www.communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.

Linkedin

SECTRA