Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

2023/0109(COD) - 24/04/2024 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 470 votes to 23, with 90 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the proposal as follows:

Subject-matter and objectives

The proposed Regulation lays down measures to strengthen capacities in the Union to **detect, prepare for and respond to cybersecurity threats and incidents**, in particular through the following actions:

- the establishment of a **pan-European network of Cyber Hubs** ('European Cybersecurity Alert System') to build and enhance coordinated detection and common situational awareness capabilities;

- the establishment of a **Cybersecurity Emergency Mechanism** to support Member States and other users in preparing for, responding to, mitigating the impact of and initiating recovery from significant, large-scale and large-scale equivalent cybersecurity incidents;

- the establishment of a **European Cybersecurity Incident Review Mechanism** to review and assess significant or large-scale incidents.

This Regulation pursues the general objectives of reinforcing the competitive position of industry and service sectors in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and of contributing to the Union's technological sovereignty and open strategic autonomy in the area of cybersecurity, including by boosting innovation in the Digital Single Market. It pursues those objectives by **strengthening solidarity at Union level**, reinforcing the cybersecurity ecosystem, enhancing Member States' cyber resilience and developing the skills, know-how, abilities and competencies of the workforce in relation to cybersecurity.

This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

Establishment of the European Cybersecurity Alert System

A pan-European network of infrastructure that consists of **National Cyber Hubs and Cross-Border Cyber Hubs** joining on a voluntary basis, the European Cybersecurity Alert System should be established to support the development of advanced capabilities for the Union to enhance detection, analysis and data processing capabilities in relation to cyber threats and the prevention of incidents in the Union.

Where a Member State decides to participate in the European Cybersecurity Alert System, it should designate or, where applicable, establish a National Cyber Hub.

National Cyber Hubs may cooperate with private sector entities to exchange relevant data and information for the purpose of detecting and preventing cyber threats and incidents, including with sectoral and cross-sectoral communities of essential and important entities. Where appropriate and in accordance with national and Union law, the information requested or received by National Cyber Hubs may include telemetry, sensor and logging data.

Cross-Border Cyber Hubs

Where at least three Member States are committed to ensuring that their National Cyber Hubs work together to coordinate their cyber-detection and threat monitoring activities, those Member States may establish a Hosting Consortium.

A Cross-Border Cyber Hub should be a multi-country platform established by a written consortium agreement. It should bring together in a coordinated network structure the National Cyber Hubs of the Hosting Consortium's Member States. It should be designed to enhance the monitoring, detection and analysis of cyber threats, to prevent incidents and to support the production of cyber threat intelligence, notably through the exchange of relevant and, where appropriate, anonymised data and information, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis and prevention and protection capabilities in a trusted environment.

Emergency mechanism

A Cybersecurity Emergency Mechanism should be established to support improvement of the Union's resilience to cyber threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant, large-scale and large-scale-equivalent cybersecurity incidents.

The Cybersecurity Emergency Mechanism should support the following types of actions: (i) preparedness actions, namely the **coordinated preparedness testing** of entities operating in sectors of high criticality across the Union ; (ii) other preparedness actions for entities operating in sectors of high criticality and other critical sectors; (iii) actions supporting response to and initiating recovery from significant, large-scale and large-scale-equivalent cybersecurity incidents, to be provided by trusted managed security service providers participating in the EU Cybersecurity Reserve; (iv) mutual assistance actions granted in the form of grants and under the conditions defined in the relevant work programmes referred to in the Digital Europe Programme.

Establishment of the EU Cybersecurity Reserve

An EU Cybersecurity Reserve should be established, in order to assist, upon request, in responding or providing support for responding to significant, large-scale, or large-scale-equivalent cybersecurity incidents, and initiating recovery from such incidents.

ENISA should prepare, at least every two years, a mapping of the services needed by the users. ENISA should prepare a similar mapping, after informing the Council and consulting EU-CyCLONe and the Commission. A response should be transmitted to the users without delay and in any event no later than 48 hours from the submission of the request to ensure effectiveness of the support action. The contracting authority should inform the Council and the Commission of the results of the process.

A **third country** associated with the Digital Europe Programme should apply for support from the EU Cybersecurity Pool where the agreement by which it is associated with the Digital Europe Programme provides for its participation in the Pool.

Evaluation and review

By two years from the date of application of this Regulation and at least every four years thereafter, the Commission should carry out an evaluation of the functioning of the measures laid down in this Regulation and should submit a report to the European Parliament and to the Council.