High common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

2022/0085(COD) - 10/03/2023 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Henna VIRKUNEN (EPP, FI) on the proposal for a regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

The committee responsible recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

Subject-matter

This Regulation lays down measures that aim to achieve a high common level of cybersecurity in Union entities. To that end, this Regulation lays down:

- obligations that require Union entities to establish a cybersecurity risk management, handling of incidents, governance and control framework;

- cybersecurity risk management and reporting obligations for Union entities;

- rules underpinning information sharing obligations and the facilitation of voluntary information sharing arrangements with regard to Union entities;

- rules on the organisation, tasks and operation of the Cybersecurity Centre for the Union entities (CERT-EU) and on the functioning, organisation and operation of the Interinstitutional Cybersecurity Board (IICB).

Risk management, handling of incidents, governance and control framework

On the basis of a full cybersecurity audit, **each Union entity** should establish its own cybersecurity risk management, handling of incidents, governance and control framework. The establishment of the framework should be overseen by the **Union entity’s highest level of management**.

The risk management framework should (i) define the strategic objectives to ensure a high level of cybersecurity in the Union entities; (ii) lay down cybersecurity policies for the security of network and information systems encompassing the entirety of the ICT environment, and define the roles and responsibilities of staff of the Union entities tasked with ensuring the effective implementation of this Regulation; (iii) include the key performance indicators (KPIs).

The framework should be **reviewed regularly** and at least every three years.

Cybersecurity risk management measures

Risk management measures should ensure a level of security for networks and information systems **across the ICT environment** that is appropriate to the risks identified in the risk management framework, taking into account the state of the art and, where appropriate, applicable European and international standards or available European cybersecurity certificates.

When assessing the proportionality of those measures, due account should be taken of the degree of the Union entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal, economic and interinstitutional impact.

The Interinstitutional Cybersecurity Board

The IICB aims to support entities in elevating their respective cybersecurity postures by implementing this Regulation. In order to support Union entities, the IICB should: (i) adopt guidance and recommendations required for Union entities' cybersecurity maturity assessments and cybersecurity plans, (ii) review possible interconnections between Union entities' ICT environments and (iii) support the establishment of a Cybersecurity Officers Group under ENISA, comprising the Local Cybersecurity Officers of all Union entities with an aim to facilitate the sharing of best practices and experiences gained from the implementation of this Regulation.

Where the IICB finds that a Union entity has not effectively applied or implemented this Regulation, it could, without prejudice to the internal procedures of the Union entity concerned: (i) request relevant and available documentation relating to the effective implementation of the provisions of this Regulation, (ii) communicate a reasoned opinion with observed gaps in the implementation of this Regulation, (iii) invite the Union entity concerned to provide a self-assessment on its reasoned opinion and (iv) issue, in cooperation with CERT-EU, guidance to bring its respective risk management, governance and control framework, cybersecurity risk-management measures, cybersecurity plans and reporting obligations.

CERT-EU mission and tasks

The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union entities, should be to contribute to the security of the unclassified environment of all Union entities and providing for them services that are analogous to CSIRTs established by the Member Sates, in particular by advising them on cybersecurity, by helping them to prevent, detect, handle, mitigate, respond to and recover from incidents. CERT-EU is an autonomous interinstitutional service provider for all Union entities, integrated into the administrative structure of a Commission Directorate-General in order to benefit from the Commission's administrative, financial, management and accounting support structures.

Reporting obligations

This Regulation lays down a multiple-stage approach to the **reporting of significant incidents**. All Union entities should report to CERT-EU any incident that has a significant impact. An incident should be considered to be significant if: (a) it has caused or is capable of causing severe operational disruption of the service or financial losses for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The Union entities should notify, inter alia, any information enabling the CERT-EU to determine any cross-entities impact, impact on the hosting Member State or cross border impact following a significant incident. All Union entities should submit to CERT-EU:

- without undue delay and in any event within **24 hours** of becoming aware of the significant incident, an early warning, which, where applicable, should indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-entity or a cross-border impact;

- without undue delay and in any event within **72 hours** of becoming aware of the significant incident, an incident report.

CERT-EU should coordinate among the Union entities the handling of **major incidents**.