A high common level of cybersecurity

2020/0359(COD) - 04/11/2021 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Bart GROOTHUIS (Renew Europe, NL) on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

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 and scope

This Directive should apply to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II who provide their services or carry out their activities within the Union. It should not apply to entities that qualify as micro and small enterprises. No later than 6 months after the transposition deadline, Member States should draw up a list of essential and important entities. This list should be updated regularly and at least every two years.

Essential and significant entities should submit at least the following information to the competent authorities: (i) name of the entity, (ii) address and updated contact details, including e-mail addresses, (iii) IP ranges, (iv) telephone numbers and (v) the relevant sector(s) and sub-sector(s) listed in Annexes I and II. Entities should inform the competent authorities of any changes to this information.

To this end, the European Union Agency for Cyber Security (ENISA), in cooperation with the Cooperation Group, should issue guidelines and templates on notification obligations as soon as possible. Processing of personal data under the Directive would be carried out in accordance with the General Data Protection Regulation (GDPR).

National cyber security strategy

The strategy should also include a framework for the allocation of roles and responsibilities of public bodies and entities and other relevant actors, a single point of contact on cyber security for SMEs, and an assessment of the general level of cyber security awareness among citizens.

Member States should also adopt:

- a cybersecurity policy for each sector covered by the Directive;

- requirements for encryption and the use of open source cyber security products;

- a policy related to maintaining the overall availability and integrity of the public core of the open Internet, including the cybersecurity of undersea communications cables;

- a policy to promote the development and integration of emerging technologies, such as artificial intelligence, into cybersecurity enhancing tools and applications;

- a policy to promote cyber hygiene, increasing general awareness of cyber security threats and best practices among citizens;

- a policy to promote active cyber defence;

- a policy to help authorities develop competences and understanding of the security aspects needed to design, build and manage connected places;

- a policy specifically addressing the ransomware threat and disrupting the ransomware business model;

- a policy, including relevant procedures and governance frameworks, to support and promote the development of public-private partnerships in cyber security.

ENISA should provide guidance to Member States to align national cyber security strategies with the requirements and obligations set out in the Directive.

Coordinated vulnerability disclosure and European vulnerability database

ENISA should develop and maintain a European vulnerability database leveraging the global Common Vulnerabilities and Exposures (CVE) registry. To this end, ENISA should adopt the necessary technical and organisational measures to ensure the security and integrity of the database.

Computer Security Incident Response Teams (CSIRTs)

Member States should ensure the possibility of effective, efficient and secure information exchange on all classification levels between their own CSIRTs and CSIRTs from third countries on the same classification level. CSIRTs should develop at least the following technical capabilities

- the ability to conduct real-time or near-real-time monitoring of networks and information systems, and anomaly detection;

- the ability to support intrusion prevention and detection;

- the ability to collect and conduct complex forensic data analysis, and to reverse engineer cyber threats;

- the ability to filter malign traffic;

- the ability to enforce strong authentication and access privileges and controls; and

- the ability to analyse cyber threats.

CSIRTs should be responsible for monitoring cyber threats, vulnerabilities and incidents at national level and acquiring real-time threat intelligence, responding to incidents and assisting entities involved, as well as contributing to the deployment of secure information sharing tools.

ENISA should publish, in cooperation with the Commission, a biennial report on the state of cyber security in the EU and submit it to the European Parliament.

Reporting obligations

Member States should establish a single point of contact for all notifications required under the Directive and other relevant EU legislation.

Essential and important entities should notify CSIRTs about significant incidents that have an impact on the availability of their service within 24 hours of becoming aware of the incident. They should notify CIRTs about significant incidents that breach the confidentiality and integrity of their services within 72 hours of becoming aware of the incident.

Fines

To ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines if the infringement was intentional, negligent or the entity concerned had received notice of the entitys non-compliance.