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

2022/0085(COD) - 22/03/2022 - Legislative proposal

PURPOSE: to establish measures to ensure a high common level of cybersecurity in the Union institutions, bodies and agencies.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: evolving technology and increased complexity and interconnectedness of digital systems amplify cybersecurity risks **making the Union administration more vulnerable to cyber threats and incidents**.

From 2019 to 2021, the number of significant incidents affecting Union institutions, bodies and agencies, authored by advanced persistent threat actors, has surged dramatically. The first half of 2021 saw the equivalent in significant incidents as in the whole of 2020.

The Centre for Cybersecurity of the EU Institutions, Bodies and Agencies (CERT-EU) has assessed the main cyber threats to which the EU institutions, bodies and agencies are currently exposed or are likely to be exposed in the foreseeable future. The analysis examined the influence of major ongoing shifts affecting the ways in which the EU institutions manage and use their IT infrastructures and services. These shifts include the increase in teleworking, the migration of systems to the cloud and the increased outsourcing of IT services.

The analysis of the 20 Union institutions, bodies and agencies shows that their governance, cyber-hygiene, overall capability and maturity vary over a broad spectrum. Therefore, requiring all Union institutions, bodies and agencies to implement a baseline of cybersecurity measures is instrumental to address this disparity in maturity and to bring all Union institutions, bodies and agencies to a high common level of cybersecurity.

This proposal builds on the EU Strategy for the Security Union and the EU’s Cybersecurity Strategy for the Digital Decade.

CONTENT: this proposal establishes a **framework to ensure common rules and measures on cybersecurity within the Union institutions, bodies, offices and agencies** to enable them to perform their respective tasks in an open, efficient and independent manner. It aims to improve all entities’ resilience and incident response capacities.

The proposed Regulation:

- obliges the Union institutions, bodies, offices and agencies to (i) establish an **internal framework** for the management, governance and control of cybersecurity risks, ensuring effective and prudent

management of all such risks, (ii) adopt a cybersecurity **baseline** to address the risks identified through this framework, (iii) carry out a cybersecurity **maturity assessment** covering all elements of its IT environment at least every three years, and (iv) adopt a **cyber security plan**;

- establishes an inter-institutional cybersecurity board to monitor the implementation of this Regulation by the Union institutions, bodies, offices and agencies, as well to supervise the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU;

- **defines the task and missions of CERT-EU** as an autonomous inter-institutional cybersecurity centre at the service of all EU institutions, bodies, offices and agencies. CERT-EU will contribute to the security of the unclassified IT environment of all Union institutions, bodies and agencies by advising them on cybersecurity, by helping them to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub;

- ensures **cooperation and the exchange of information among CERT-EU, and the Union institutions**, bodies and agencies to develop trust and confidence. To this end CERT-EU may request Union institutions, bodies and agencies to provide it with relevant information and CERT-EU may exchange incident-specific information with Union institutions, bodies and agencies to facilitate detection of similar cyber threats or incidents without the consent of the affected constituent. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the affected constituent;

- obliges all EU institutions, bodies, offices and agencies to **notify CERT-EU** of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them.

Budgetary implications

According to studies, direct cybersecurity spending has tended to vary between 4 and 7% of the aggregated IT expenditures of organisations. However, the threat analysis undertaken by CERT-EU in support of this legislative proposal indicates that international bodies and political organisations face increased risks and therefore a level of 10% of IT spending on cybersecurity would seem a more adequate target.

The exact cost of such efforts cannot be determined due to the lack of detailed information on IT expenditure of the Union institutions, bodies and agencies and the relevant share of cybersecurity spending.

CERT-EU will require additional resources to fulfil its expanded role and these resources should be reallocated from the Union institutions, bodies and agencies benefitting from CERT-EU’s services.