EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)

2017/0225(COD) - 30/07/2018 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Angelika NIEBLER (EPP, DE) on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

The committee recommended that the position of the European Parliament adopted at first reading following the ordinary legislative procedure amend the Commission proposal as follows:

Mandate and tasks of the Agency: the EU Cybersecurity Agency shall be reinforced for the purpose of: (i) contributing to achieving a high common level of cybersecurity; (ii) preventing **cyber-attacks** within the Union; (iii) **reducing fragmentation in the internal market** and improve its functioning; (iv) ensuring consistency by taking into account the Member States' cooperation achievements under the Directive on security of network and information systems (NIS Directive).

The Agency shall **respect the competences of Member States** regarding cybersecurity, especially those concerning public security, defence, national security and the activities of the state in areas of criminal law.

The main tasks of the Agency shall be, *inter alia*, to:

- promote **cooperation, coordination and information sharing** at Union level among Member States, Union institutions, agencies and bodies, and relevant stakeholders, on matters related to cybersecurity;
- support projects contributing to a **high level of awareness, cyber hygiene and cyber literacy** among citizens and businesses on issues related to the cybersecurity;
- **contribute towards raising the awareness of the public**, including by promoting education, about cybersecurity risks and provide guidance on good practices for individual users aimed at citizens, organisations and businesses;
- assist Members States and Union institutions in establishing and implementing **coordinated vulnerability disclosure policies** and government vulnerability disclosure review processes, whose practices and determinations should be transparent and subject to independent oversight;

- facilitate the establishment and launch of a **long-term European IT security project** to support the development of an independent IT security industry across the Union;
- support **operational cooperation** among Member States, Union institutions, agencies and bodies, with a view to achieving collaboration, by analysing and assessing existing national schemes, by developing and implementing a plan and by using the appropriate instruments to achieve the highest level of cybersecurity certification in the Union and the Member States;
- contribute to **an EU level response** in case of large-scale cross-border cybersecurity incidents and crises, mainly by supporting the technical management of incidents or crises with the aid of its independent expertise and its own resources;
- organise **at least once a year**, cybersecurity exercises across the Union.

Organisation and management: Members suggest that ENISA further strengthens its capabilities and technical expertise to be able to provide adequate support for operational cooperation with Member States. For this purpose the Agency shall **progressively reinforce its staff** dedicated to this task so as to be able to collect and analyse autonomously different types of a wide range of cybersecurity threats and malware, perform forensic analysis and assist Members States in the response to large scale incidents.

ENISA shall increase its know-how and capacities based on existing resources present in the Member States, notably by seconding national experts to the Agency, creating pools of experts, and staff- exchange programmes.

The Agency shall set up an **ENISA Advisory Group** composed of recognised security experts representing the relevant stakeholders, such as the ICT industry – including SMEs, operators of essential services according to the NIS Directive, providers of electronic communications networks or services available to the public, consumer groups, academic experts in the cybersecurity, **European Standards Organisations** (ESOs), and EU agencies.

The ENISA Advisory Group shall set out the objectives in its **work programme**, which shall be published every six months to ensure transparency.

The Agency shall also have a **Stakeholders Certification Group** as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations, academia and other relevant stakeholders.

European cybersecurity certification schemes: Members consider that not only products and services should be covered by the regulation, but also **the whole life cycle**. Thus, **processes** have also to be included in the scope of application.

The certification scheme shall ensure:

- the confidentiality, integrity, availability and privacy of services, functions and data;
- that services, functions and data can be accessed and used only by authorised persons and/or authorised systems and programmes;
- that a process is in place to identify and document all dependencies and known vulnerabilities in ICT products, processes and services;
- that ICT products, processes and services are secure by default and by design;
- that other risks linked to cyber-incidents, such as risks to life, health, the environment and other significant legal interests are minimised.

Members suggested greater involvement from Member States and industry in the certification process.

The Agency shall maintain **a website** with all relevant information on European cybersecurity certification schemes, including with regards to withdrawn and expired certificates and national certifications covered, and ensure that they are made public.

Lastly, to promote the overall acceptance of certificates and conformity assessment results issued by conformity assessment bodies, Members proposed that national certification supervisory authorities operate a rigorous and transparent **peer evaluation system** and regularly undergo such evaluation.