FEDIL

Position

POSITION OF FEDIL – CYBERSECURITY ACT

This position paper constitutes FEDIL's contribution to 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 »).

On 19th of September 2017, the European Commission adopted a cybersecurity package, which builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response. As part of this package, the Commission presented a new proposal on cybersecurity, based on two pillars, concerning the reform of ENISA and the establishment of an EU Cybersecurity Framework.

CONTEXT

With an increasing number of activities and services being online nowadays, the digitisation of industry and the rising number of connected devices (Internet of Things), the role of cybersecurity has become crucial to provide a stable digital economy and to ensure consumers' trust. Indeed, "around 28 billion connected devices are expected by 2021"[1].

According to CCIPS "more than 4,000 ransomware attacks at the European level} have occurred every day since the beginning of 2016" (a 300% increase year over year). Those attacks have evolved from being perpetrated by individuals to being highly sophisticated and attributed to organised crime. The economic impact of cyber-crime, compromising the functioning of our economy, society and trust in a fully connected market, is alarming and won't stop its exponential rise.

With 7000 incidents registered solely in 2017[2], and considering Luxembourg's significant investments over the last few years into areas such as Tier IV data centres, European High-Performance Computing, Internet of Things, smart mobility and smart buildings, cybersecurity has become a strategic priority for the Grand-Duchy's political and socio-economic development.

Altogether, these elements and the prospect of large-scale incidents demonstrate how a European approach on cybersecurity is essential not only for Luxembourg but also for the European Union as a whole.

General comments

FEDIL welcomes the "Cybersecurity Act", which will contribute to the good functioning of the European Digital Single Market and guarantee a highly qualitative cybersecurity environment.

Cybersecurity is a common societal challenge and should be a collective responsibility. The Commission's objectives to strengthen the EU cybersecurity industry and to increase the Member States' capabilities by improving the European cooperation while mainstreaming cybersecurity policies as well as behaviours at every level of the value chain, are praiseworthy.

Given the ubiquitous nature of cybersecurity, a regulatory framework and full harmonisation to assert effectiveness and to prevent fragmentation is needed. Rather than individual actions, a collective effort will benefit the EU's resilience and defence in cybersecurity.

Specific comments

ENISA'S new role should be explicit

Despite the ever-increasing role of IT-related concerns in Europe, ENISA's role has mainly been to provide expertise and advice rather than dealing operationally with cybersecurity. Giving ENISA a permanent mandate with operational tasks is paramount in improving cybersecurity throughout the EU.

FEDIL endorses the re-evaluation of ENISA's role. Becoming the EU Agency for cybersecurity, ENISA's responsibilities will be reinforced through increased **financial and human resources**. Indeed, to assist Member States and industry in an effective manner, a substantial effort in terms of resources, talent and time is needed.

ENISA's mission to exchange best practices in the Cooperation Group and to offer *"trainings regarding cybersecurity, where appropriate, in cooperation with stakeholders"* (article 6.1. (h)), is valuable. However, our members believe the proposed regulation could allocate ENISA even more **appropriate means to raise awareness** on cybersecurity. Article 6.1 (g) limits the Agency's assistance to the organisation of *"yearly large-scale cybersecurity exercises at the Union level {and the preparation of} policy recommendations based on the evaluation process and lessons learned"*. In our view, ENISA should give Member States and stakeholders more incentives for participating in these exercises.

The results of such exercises should be promoted and documented in order to better inform businesses and citizens and to better assess their level of preparedness in the event of future cyberattacks.

Furthermore, the "Cybersecurity Act" will put in place a **level-playing field** for businesses and an **EU reference framework with common ground rules**. Since there are already centres of competences in the USA or in Israel, it is essential for ENISA to promote EU practices internationally. These reference points are decisive to attract investment from global companies.

ENISA should be an Operational Cooperation point

We welcome that the "Cybersecurity Act" foresees an operational cooperation at the European level. The Agency should be the central coordination point with all relevant bodies for operational efficiency. To assure effective cooperation, an **adequate governance model** between ENISA and the existing cybersecurity national agencies (ANSSI, BSI, GOVCERT.LU etc.) is needed. Failure to comply with this governance model would favour the creation of a "bureaucratic monster"[3].

The proposal foresees that national certification authorities contribute to the elaboration of certification requirements as they participate in the European Cybersecurity Certification Group. This Group *"assists, advices and cooperates with ENISA in the preparation of a candidate scheme"* for the cybersecurity certification (article 53.3 (b)). In this respect, the role of national security and certification authorities should be clarified. They should not be turned into mere "check-in counters", under ENISA's authority.

Cybersecurity Information Sharing (article 7.2) within and across industries is essential to safety, security, and resilience. To build the necessary trust, businesses should be given more legal certainty when sharing cyber-intelligence with other public and private entities.

Additionally, we would like to insist on the need to further strengthen international cooperation so as to avoid the formation of "standard-blocks" to guarantee the coherence of international processes and to generally prevent trade barriers.

The new EU cybersecurity certification framework should be a collective effort

FEDIL welcomes the EU Certification Framework's aim to build up consumers' trust and to improve the security of ICT products and services.

Our members support an EU Framework, establishing the **primacy of European cybersecurity certification schemes** over national schemes and thus, preventing the fragmentation of the European market. Such an EU level harmonisation would facilitate cross-border business and lower unitary compliance costs, which is essential for European companies, including SME's and start-ups.

Likewise, the idea of **mutual recognition** of national initiatives where EU level criterions are not deemed beneficial, has to be encouraged.

We support a **"one-stop-shop" for certification,** where businesses will only have to certify their products or services once and obtain a certificate valid in every Member State, This form of certification should follow a "security by design" approach, promoting responsible innovation and include the "privacy by design" principle in order to be compliant with the General Data Protection Regulation[4].

However, we regret that the proposed regulation doesn't refer to any form of market surveillance, which is necessary to guarantee the good functioning of the EU Cybersecurity Certification Framework.

Pragmatic certification Schemes

FEDIL endorses the three assurance levels (basic, substantial, high) suggested by the Commission. as they strike the right balance between different protection profiles and the need to adopt a broad and general notion of cybersecurity.

Requirements of ICT products and services should be further specified in the national certification schemes, for example by adding references to standards or technical specifications.

Yet, **a strict "one-size fits all"** certification scheme would be unacceptable. It is crucial for certification schemes to reflect the various maturity levels of different markets and security requirements should consider the product and services' equipment, processes and risks.

Our members support a **mandatory review of certifications every three years** since certifications, unlike labels, are an ongoing and continuous improvement process.

A bottom-up approach for the establishment of cybersecurity schemes

FEDIL is in favour of **a "bottom-up approach"**, which would allow the industry to contribute with specific knowledge and expertise to the design of adapted assurance levels and security requirements. Existing certification schemes and good practices should be integrated into the establishment of EU certification schemes as to prevent national and local cybersecurity standards to be raced to the bottom. In this context, Luxembourg should promote its electronic archiving system on a European level.

Moreover, it is important that ENISA actively and on a permanent basis, participates in international stakeholder meetings in order to defend European interests regarding normalisation, standardisation and certification.

A voluntary certification

The scope of the "Cybersecurity Act" being very broad, the certification framework has to operate on a voluntary basis. Allowing businesses to further use international certification models when these seem more adapted to their services and products (e.g. ISO or ISAE third-party assurance reports on effectiveness of internal controls) is of great importance.

A rigid and mandatory approach may hamper innovation and significantly increase costs for businesses, mostly for SME and start-ups. In a fast-changing market, flexibility is central as it is likely that certifications will implicitly become mandatory for a given industry via market-driven self-regulation.

FOOTNOTES

1. Ericsson Mobility Report, November 2017, in: https://www.ericsson.com/assets/local/news/2016/03/ericsson-mobility-report-nov-2015.pdf
2. CIRCL – https://circl.lu/opendata/statistics/
3. Quote Head of Digital Task Force, BusinessEurope
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)