Council of European National Top-Level Domain Registries

Brussels, Belgium
26 November 2018

CENTR Board Statement on the EU Cybersecurity Act

Introduction

CENTR is submitting the following comments 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 (the ''Cybersecurity Act'', hereinafter the Proposal).

CENTR is the association of European country code top-level domain (ccTLD) registries. All EU Member State and EEA country ccTLDs (including .eu) are members of CENTR.

CENTR represents the industry that is at the core of public internet, safeguarding the stability and security of the internet as we know it today. ccTLD registries are listed as “operators of essential services”, as enshrined in Annex II of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). As such, the Proposal and a possible mandatory certification scheme supported by the European Parliament in its respective Report[1] might have a significant influence on the day-to-day operation of a ccTLD registry.

Areas of concern to CENTR members

CENTR members are concerned about the potential impact of the mandatory EU certification scheme that has been proposed by the Report of the European Parliament (Recital 58 (a) of the Report): “The **mandatory use of European cybersecurity certification by operators of essential services** should be restricted to those elements that are critical for their functioning[...]”. Article 48a of the Report obliges the European Commission to compile a list of categories, products and processes that might be subject to a possible mandatory certification scheme. Although Article 53(3)(f a) of the Report recognises the need to align European cybersecurity schemes with internationally recognised standards, it is nevertheless important to stress the necessity to avoid duplicating the efforts made at international level.

[1] European Parliament, Committee on Industry, Research and Energy, Report 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") (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)), 30.07.2018

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium

Phone: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org

www.centr.org

ccTLDs are aware of and widely use international standards when it comes to cybersecurity. Some of the most widely-recognised information security standards amongst European ccTLDs are published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO standards are widely recognised across ICT industries, and its uptake in Europe is steadily growing.[2]

The current Information Security Management System (ISMS) standard series consists of coherent standards, some already published and some still under construction. They contain a number of important structural components such as:

- Standards describing requirements on an ISMS (ISO/IEC 27001)
- Requirements for bodies certifying compliance with ISO/IEC 27001 (ISO/IEC 27006)
- Additional requirements for sector specific performance of information security management systems (ISO/IEC 27009)

In addition, there are several other ISO standards related to or complimentary to ISO 27000 family standards: e.g. ISO/IEC 27032 ("Guideline for cybersecurity"), ISO 22301 ("Societal security - Business continuity management systems – Requirements") and ISO 31000 ("Risk Management").

Furthermore, it is noteworthy that information security is not solely a matter of certification (i.e. ISO 27001) and is complemented by other voluntary industry practices and security standards, such as Internet Standards issued by the Internet Engineering Task Force (IETF) that relate to security on all levels of the internet infrastructure.

The Explanatory Memorandum to the Proposal from the European Commission states that "[...]the landscape of cybersecurity certification of ICT products and services in the EU is quite patchy", making that assumption based on the brief assessment of one international standard: ISO 15408, and without considering any other industry standards in the field. Based on this brief assessment provided by the European Commission, it is too far-fetched to make conclusions about the (in)effectiveness of internationally-recognised global standards when it comes to cybersecurity, and a more fact-based approach is needed. It typically takes decades to develop and adopt new frameworks, which are also highly costly. A more natural and commonly accepted first step might be to adopt the self-declaration of conformity, which has proved to work rather well in practice.

CENTR members recognise the need to promote standardisation efforts in the sphere of cybersecurity, which is becoming increasingly prominent with the advent of new technology. However, it is essential to recognise the efforts made at global level and to adequately respond to these practices through legislation, without disrupting the industries which are already well-established at the core of the internet infrastructure. In its initial Proposal, the European Commission had recognised the need for a *voluntary EU certification scheme,* in order to mitigate the risks of administrative burden and higher costs. Additionally, the Proposal and the Report call for collaboration between the European Union Agency for Network and Information Security (ENISA; hereinafter "the Agency"), Member States and the industry, to draw up

[2] International Standardization Organization, ISO Survey of certifications to management system standards – ISO/IEC 27001 – data per country and sector 2006 to 2017

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

guidelines regarding the technical areas related to security requirements for operators of essential services, **regarding already existing standards** (Article 8(b) of the Proposal).

CENTR members welcome the need to establish the Stakeholder Certification Group as enshrined in Article 20a of the Report and the inclusion of representation by operators of essential services in the advisory group to the Agency – the Permanent Stakeholder Group (Article 20 of the Proposal). It is necessary to include all affected stakeholders in the process of establishing the EU cybersecurity certification scheme to make sure the latter is not developed in information silos. This also includes the cooperation with international standardisation bodies.

Recommendations

- CENTR members call for co-legislators to remain strongly aligned with globally recognised international – both formal and de facto - standards and already-existing certification practices when it comes to the operation of a ccTLD as an essential service in light of the EU Cybersecurity Act, and to make sure that the proposed EU certification scheme follows already-existing and well-established industry practices in cybersecurity on a global level.
- CENTR members call for co-legislators to ensure that operators of essential services affected by the EU certification scheme (including ccTLDs) are adequately represented in the advisory groups to the Agency and that they be closely consulted during the preparations of the EU cybersecurity certification scheme.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org