IT Security:

CLUSIT and Information Security & Privacy Osservatorio introduce their perspective

Gabriele Faggioli

November 27th, 2017

OSSERVATORI.NET digital innovation

Clusit

Clusit Education

Clusit
Osservatori Politecnico of Milan

CLUSIT, the Italian Association for Information Security, is, to date, the most authoritative and numerous association on the Italian scene, whose objectives are to **defend** and **promote** the **culture of information security** not only among companies and the Public Administration, but also with regard to citizens. In addition, the purpose of the CLUSIT is **to participate in the drafting of laws, rules and regulations with regard to cyber security at both national and European level.**

The **Osservatorio of the Politecnico of Milan** have been set up within the Politecnico in order to **produce** and **broadcast knowledge** about the **opportunities** and **impacts** that **digital technologies** have on businesses, public administrations and citizens. All this through research, correct communication and adequate training.

Introduction

- The value of certification scheme is based on two main conditions:
  - good and services suppliers must be available to adopt the scheme
  - purchasers must recognize the value of the scheme.

- Both good practices and the recent European legislation set these targets based on risk mitigation, and not just on assurance levels.

- Even more, cybersecurity today is one of the factors that a prepared customer values when purchasing products and services.

- The risk related to IoT security, both for companies and for the citizens, need to be addressed at an European or global level.
- A certification scheme dealing with this risk could surely help.

- The cybersecurity is daily evolving together with new technologies (and new attacks): this requires strong research and greater investments on innovation aspects.

Introduction

The proposal of *"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")"*

It provides for a series of **measures** to **avoid** and **prevent** possible **fragmentation** of cybersecurity certification systems in the EU.

It introduces a **comprehensive framework of rules** governing European cyber security systems.

At present, however, the European landscape of cybersecurity certifications of ICT products and services is rather diverse and fragmented.

This situation leads to a constant increase in costs and represents a considerable administrative and economic burden for companies operating in more than one Member State.

Art. 43 – European cybersecurity certification schemes

Article content

«A European cybersecurity certification scheme shall attest that the ICT products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and systems.»

Note

The recent approach of the European legislation, along with industry technical standards (eg. ISO 27001:2013), focuses on **risk mitigation** rather than on the definition of specific technical measures to ensure a certain assurance level.

- **ENISA** should therefore **cooperate with several user category representative** (eg EBA and EBF for banking sector) to define a consistent set of "protection profiles" to mitigate the risk for different categories of users (citizens, companies) and applications. Such set should include gradually different features, consequently increasing the level of assurance, so that a supplier can cover the greatest possible number of user classes and applications with just a certification.
- A different setting as such would clearly result in an extensive changes to the text. Classes of users should include at least "Operators of Essential Services" and "Digital Service Providers - DSPs" specified in the NIS Directive.

Even considering the widespread use of the term "***cybersecurity***", it is worth pointing out that its proper and exact meaning is not commonly shared; therefore, with regard to certification, the Commission should ensure that any use of such a term does not give rise to ambiguity in the scope, objectives or effectiveness of this certification.

Art. 44 - Preparation and adoption of a European Cybersecurity Certification Scheme

Article content

«Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.»

Note

- How **ENISA** can draw a "scheme" using existing technical standards and best practices, is unclear; perhaps from the latter could be derived "protection profiles“, in according to the **Common Criteria**, that can be adopted in case of risk profiles linked to different types of users and applications.

Art. 45 - Security objectives of European cybersecurity certification schemes

Article content

«A European cybersecurity certification scheme shall be so designed to take into account, as applicable, the following security objectives:

(a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure;

(b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, accidental loss or alteration;

(c) ensure that authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;

(d) record which data, functions or services have been communicated, at what times and by whom;

(e) ensure that it is possible to check which data, services or functions have been accessed or used, at what times and by whom;

(f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;

(g) ensure that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates.»

Note

The **list** of **threats** and **security features** identified in this proposal is not exhaustive. Generally, the introduction of such lists can generate rigidity and updating difficulty which would be better to prevent.
It is difficult for these lists to be really exhaustive or not misinterpreted. ENISA would be better to take charge of these technical aspects, as ESMA with regard to (EU) Regulation No. 600/2014 (MIFID2).

Art. 46 – Assurance levels of European cybersecurity certification schemes

Article content

«A European cybersecurity certification scheme may specify one or more of the following assurance levels: basic, substantial and/or high, for ICT products and services issued under that scheme

The assurance levels basic, substantial and high shall meet the following criteria respectively:

(…)»

Note

Defining a scheme as outlined above seems to be challenging since currently there are only product certification schemes and not services certification schemes with assurance levels.

The problem could be overcome by referring to risk profiles and relevant security profiles, instead of generic levels whose usefulness in many contexts would be doubtful.

- The definitions of the various **assurance levels** provided are linked to a single non-quantitative criterion that is likely to be interpreted in a number of different ways. The same problem has occurred in other cases (eg. for eID and ISO 29115, which likewise apply general terms).
- Assurance levels should be linked to the kind of cyber attacker to face with, the residual risk level they should lead to and/or other measurable or concrete factors. This aspect would also be overcome by referring to risk and protection profiles.

Art. 47 – Elements of European cybersecurity certification schemes

Article content

«A European cybersecurity certification scheme shall include the following elements:

(a) subject-matter and scope of the certification, including the type or categories of ICT products and services covered;

(…)»

The ability to support the activities of "Identify, Protect, Detect, Respond and Recover" of service users or product users (Framework for Improving Critical Infrastucture Cybersecurity - NIST, National Institute of Standards and Technology)

Note

- (a) Since it comes to products, the version must be included.
- The ability to integrate with customer accidents management processes, albeit with different modes depending on the type of service or product, should be included in the scope of certification.

Art. 53 – European Cybersecurity Certification Group

Article content

«The European Cybersecurity Certification Group (the 'Group') shall be established.

The Group shall be composed of national certification supervisory authorities. The authorities shall be represented by the heads or by other high level representatives of national certification supervisory authorities.»

Note

In the Group should be also represented **ESO** (*European Standardization Organizations*) as defined in EU Regulation n. 2012/1025 which are not included in this article of the Proposal.

Art. 54 – Penalties

Article content

«Member States shall lay down the rules on penalties applicable to infringements of this Title and European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall [by …/without delay] notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.»

Note

- As a **voluntary scheme**, it is not clear "what and who" should be penalized.
- However, it would be desirable for penalties to be at least provided for certifying entities if the latter certify a product or service without the characteristics required. This because the certification is paid by the certified one and this creates a conflict of interests that heavily affects the whole certification process.
- It would be useful to foresee that **ENISA** may audit certified products and services (without however having a specific burden for which it would not have the resources or capabilities). Participants who have been considered for assurance profile (eg. EBA and EBF), those really interested in the quality of the result, should also be permitted to participate in the audit.

Proposal of a Regulation and existing certification bodies and schemes

The following slides concern some problems encountered in the relationship between the Proposal for a Regulation and the various entities (eg. national accreditation bodies), as well as inappropriate references to existing standards.

Art. 44 - Preparation and adoption of a European Cybersecurity Certification Scheme

Article content

«(…) ENISA shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes.»

Note

This is already a task for **national accreditation bodies** and for **european accreditation bodies**. It should be reworded to avoid any overlaps among tasks.

Art. 48 – Cybersecurity certification

Article content

«By the way of derogation from paragraph 3, in duly justified cases a particular European cybersecurity scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body. Such public body shall be one of the following:

(…)

(c) a body established under laws, statutory instruments, or other official administrative procedures of a Member State concerned and meeting the requirements for bodies certifying products, processes and services further to ISO/IEC 17065:2012.

(…).»

Note

(c) it would be appropriate to modify the reference to ISO ISO/IEC 17065 only, especially if different schemes need to be integrated. It should be mentioned, at least, to ISO/IEC 17021 and ISO/IEC 17024 or consider an higher level.

Art. 49 – National cybersecurity certification schemes and certificates

Article content

«Without prejudice to paragraph 3, national cybersecurity certification schemes and the related procedures for the ICT products and services covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant Article 44(4). Existing national cybersecurity certification schemes and the related procedures for the ICT products and services not covered by a European cybersecurity certification scheme shall continue to exist.»

Note

The article should be **revised or deleted** as it would undermine the extent of the existing certifications (see ISO/IEC 27001) and for certified organizations. It also prevaricates the institutional prerogatives of the national accreditation bodies.

Art. 50 – National certification supervisory authorities

Article content

«Each Member State shall appoint a national certification supervisory authority.

Each Member State shall inform the Commission of the identity of the authority appointed.

Each national certification supervisory authority shall, in its organization, funding decisions, legal structure and decision-making, be independent of the entities they supervise.

*Member States shall ensure that national certification supervisory authorities have adequate resources to exercise their powers and to carry out, in an effective and efficient manner, the tasks assigned to them.*ti.

(…)

National certification supervisory authorities shall cooperate amongst each other and the Commission and, in particular, exchange information, experiences and good practices as regards cybersecurity certification and technical issues concerning cybersecurity of ICT products and services.»

Note

The risk that this article entails is to **duplicate the role of national accreditation bodies**, which should be automatically entitled to perform these tasks, with considerable cost savings and increased efficiency.

Conclusion

In conclusion, the content drawn up by European legislators of this Proposal for a Regulation is, without any doubt, commendable.

However, in the light of the above, it is considered necessary to make some changes to the text of the Proposal for a Regulation and, in particular, to the following aspects:

- *adopt a **different approach** based on risk mitigation rather than specific technical measures to ensure a certain level of assurance;*
- *define **levels of assurance for certification schemes** that are not generic, but refer to specific risk profiles and related protection profiles;*
- *from a **penalties point of view**, it would be appropriate to clarify "what and who" should be sanctioned, providing at least that these should be addressed to certifying bodies;*
- *provide that **ENISA** may carry out an **audit activity** on certified products and services in which the subjects for whom the authorization profile has been designed may also participate.*

Thanks for your attention!

faggioli@mip.polimi.it