PRESS RELEASE

Requirements on a future European ICT Security Certification and Labelling Framework: TeleTrusT - IT Security Association Germany criticizes plans of the EU Commission and calls for amendments

Berlin, October 04, 2017 - The European Commission has published a regulation proposal, also concerning a European ICT Security Certification and Labelling Framework to improve the security properties of products, systems and services already in the design phase ("security by design"). The intentions behind this regulation are noble since it is desirable to increase the protection of citizens and businesses through better cyber security awareness and practices. However, this proposal has serious technical flaws and lacks also the openness and transparency that can be expected from setting standards used to support EU legislation.

https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

TeleTrusT positions:

The proposal is regarded to be a necessary and fundamental contribution for cyber security in digital infrastructures as the development and deployment of new digital technologies with their increasing inherent risks require a sustainable framework to provide appropriate technical standards and certification services in the "Digital Single Market". This will lead to secure products, systems and services already before they enter the market and during their complete lifecycle.

The proposal seeks to give complete power to the European Commission to decide what cyber security schemes are required within the EU, which standards apply to a scheme, and what types of products or services are covered by a scheme. A scheme could cover smart meters, IoT wearables, databases, cloud, smartphones, etc., in fact any ICT product. If there are no applicable standards for a scheme, the requirements that are to be met to certify against a scheme will be baked into the scheme itself without requiring consultation.

The proposal has the EU Agency for Network and Information Security (ENISA) at the heart of writing the schemes, but the ultimate decision of when a new EU scheme is required, what products and services are covered, and on a scheme's final content rests solely with the Commission. There is no involvement of Member States, the European Council, the European Parliament, National Standards Bodies, societal stakeholders, or industry. While initially a scheme will be voluntary to use, this is a weak argument in defense of a regulation that gives too much power to the European Commission.

The new framework can only be successful under the following conditions:

1. The Framework migrates existing certification infrastructures without disruption of business, especially SOGIS-MRA ("Senior Officials Group Information Systems Security - Mutual Recognition Arrangement", with currently 14 Member States, competent schemes and private evaluation labs, initiated by the European Commission in the early nineties, with significant recognition by the industry and a world market position).

2. Certification shall rely on open standards, permit competition between labs and schemes and between the most appropriate security solutions for a defined security problem.

3. The Framework can produce results at the speed of the technological change and satisfy market needs in time and efficiency.

4. An efficient relationship between the Framework and the European Standardisation Organisations can be established.

…

5. As far as ICT security aspects are concerned the European Commission´s directives or regulations for any vertical digital market will consider the requirement for appropriate technical security standards and certifications and involve the Certification Board accordingly and on a regular basis. If a vertical sector cannot be harmonised then harmonisation of technical standards and certification will be hard to achieve.

IT Security is also a concern of network security, public and national security and digital sovereignty. IT Security is not only a concern of the Digital Single Market but also of the Member
States. This is especially the case for crypto standards and the qualification of evaluation labs.

Therefore, a future European ICT Certification and Labelling Framework should:

1. establish a "European Cyber Security Certification Board" composed by representatives of the Member States in liaison to the ESO, the European Data Protection Board (EDPB) with the responsibility to define its terms of references and establish working groups,

2. support the Commission DGs when developing communications, directives and regulations for vertical sectors so that standardisation and certification is prepared at a very early state and can provide synergies between the vertical digitalisation sectors,

3. migrate SOGIS-MRA from a Member States driven activity to a pan-European one,

4. keep the independence of standardisation and evaluation by providing an appropriate accreditation system for the labs and enhance the accreditation regulation by including an additional sector-specific exception according to recital No. 5 in 765/2008,

5. establish a role for ENISA to provide the secretariat and organisational infrastructure for the (new) European Cyber Security Certification Board,

6. support member states and industry to initiate innovations for better IT security and to create a level playing field for European industry in the world market.

TeleTrusT - IT Security Association Germany, Dr. Holger Muehlbauer, Managing Director, Phone: +49 30 /40054310, holger.muehlbauer@teletrust.de
www.teletrust.de