Position Paper on the EU Commission's proposal for a Cybersecurity Act

February 2018

DIN e.V.

An DIN-Platz
Burggrafenstraße 6
10787 Berlin
Germany
www.din.de

Contact:

Sibylle Gabler
Head of Government Relations
Phone: 030 2601-1112
Fax: 030 2601-1115
E-Mail: sibylle.gabler@din.de

DKE

Stresemannallee 15
60596 Frankfurt
Germany
www.dke.de

Contact:

Bernd Schwarzzenberger
Senior Principal Expert External Relations
Phone: 069 6308-298
Fax: 069 6308-9298
E-Mail: bernd.schwarzzenberger@vde.de

Synopsis

- Prevent a patchwork of national solutions: Progress towards EU-wide harmonization!
- Do not create a parallel system: Apply the better regulation technique of the New Legislative Framework for Cybersecurity!
- Avoid confusion in the marketplace: Make use of market-driven, consensus-based European and international standards!

****

DIN and DKE welcome the proposal made by the European Commission for a *Cybersecurity Act [COM (2017) 477]* as it aims at preventing different national solutions. In this regard, DIN and DKE invite the legislator to build the Act on the already existing successful New Legislative Framework (NLF) that facilitated the European single market and benefits of international and European Standards.

Progress towards EU-wide harmonization

DIN and DKE welcome the plan to define European cybersecurity certification schemes on the European level. This will prevent fragmentation due to a patchwork of national solutions in Member States.

In case of missing international or European Standards the European Commission should mandate ESOs to develop them towards EU-wide harmonization.

Apply the better regulation technique of the New Legislative Framework for Cybersecurity

The governance described in the Commission's proposal on Cybersecurity is at odds with the principles of better regulation. There is no adequate provision for stakeholder participation in the decision-making structures which will bring about the new certification schemes, although it is the stakeholders whose products bear or apply the certificates. Regulatory approaches only fulfil their goal of relieving the state of its regulatory burden if they concentrate on formulating essential requirements and make reference to international/European standards.

The New Legislative Framework has proven its value and positive impact in successfully providing a clean allocation of tasks between legislation, standardization and conformity assessment for regulating the safety and performance of goods, systems, and services within the European Union. A cybersecurity regulation should therefore be integrated into the NLF instead of establishing a parallel system which would create red tape and confusion in the marketplace. The Framework has sufficiently proven its capacity of securing safety and performance and involving relevant stakeholders while being continuously open to innovations.

Therefore the Cybersecurity Act needs to be formulated in a way to

- Define cybersecurity requirements that are essential in a similar way to market access requirements in the context of the NLF.
- Decide on to what extent harmonized European Standards could be used for complying with these requirements, including a respective declaration of conformity and presumption of conformity.
- Fill gaps for fulfilling essential requirements by request for standards to the European Standardization Organizations according to Regulation 1025/2012.
- Formally involve the European Standards Organizations (CEN, CENLEC, and ETSI), the National Standards Bodies, and thereby stakeholders from industry and society in order to tackle the challenges ahead.

A cybersecurity certification framework should refer to technical requirements without preference to specific solution or components. Hence it must be based on international standards that create a uniform, comparable, practicable and technically proven foundation. Thus, market participants are able to select the best suitable technical realization. This will spur further development and innovation.

Furthermore a cybersecurity framework should also cover the processes of IT-system integration and IT-system operation in order to foster and support decision-making, especially of SMEs that depend on IT service providers.

Use a risk-based approach and define different security levels

Missing cybersecurity would be a crucial factor for endangering the success of the digital economy. It is important to distinguish between different threat scenarios and risks from the perspective of end users, economy, and especially operators of critical infrastructures.

Article 46 of the proposed Cybersecurity Act foresees three different assurance levels. Missing however is the perspective of a risk-based approach. Governments, critical infrastructure, businesses and consumers face different vulnerabilities and risk levels. Hence they need different requirements and solutions.

Therefore, different security levels should be defined according to the need of users for trust and confidence based on International Standards.

Understand cybersecurity as an international challenge that can be tackled with international standards

For all activities by European Commission, Member States, or industries, international and European standardization is a key instrument. Security standards define requirements, support open markets, boost the internal market and reduce transaction costs.

International Standards provide the basis on which our export-driven industry can access global markets. The Cybersecurity Act must aim at preventing the fragmentation of specifications, not only within Europe but also globally. Therefore, any framework should

take into account existing and already widely accepted standards[1] and conformity assessment schemes.

The European Standardization Organizations CEN and CENELEC have set up the new joint committee "Cybersecurity and Data Protection" (JTC 13) in order to transpose international standards into European Standards taking into account European legal requirements derived from NIS and GDPR.[2]

Vice versa, there is the chance to internationalize a European approach – which might offer a higher level of security – via the international standardization organizations.

European and international standards developed in a full consensus process, must form the basis for conformity assessment. This guarantees openness as well as broad stakeholder participation, and leaves room for future innovations.

Digitization is of global nature, cybersecurity threats do not stop at borders. Any standardization initiative at the European level should first reflect the global work of International Standardization Organizations.

About DIN

DIN, the German Institute for Standardization, is the independent platform for standardization in Germany and worldwide. As a partner for industry, research and society as a whole, DIN plays a major role in paving the way for innovations to reach the market and advancing progress in innovative areas such as Industry 4.0 and Smart Cities. More than 32,000 experts from industry, research, consumer protection and the public sector bring their expertise to work on standardization projects managed by DIN. The results of these efforts are market-oriented standards and specifications that promote global trade, encouraging rationalization, quality assurance and environmental protection as well as improving security and communication. For more information, go to www.din.de

About DKE

The DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE as a joint organization of VDE and DIN is the national organization responsible for the compilation and maintenance of standards and safety specifications covering the areas of electrical engineering, electronics and information technology in Germany. It actively represents German interests in the European Committee for Electrotechnical Standardization (CENELEC) and in the International Electrotechnical Commission (IEC). The DKE maintains close links to ETSI and implements ETSI European Standards in the German standards collection. About 5 500 technical experts from industry, science and administration are organized in the DKE. Electrotechnical safety standards elaborated in the DKE as VDE Specifications are part of the VDE Specifications Code of safety standards.

---

[1] Such as the requirements and information security management for IT (ISO/IEC 27000 series), industrial automation and control systems (IEC 62443), ISO 15408 (Evaluation criteria for IT security)and industry sector-specific standards. Furthermore for the evaluation and assessment of processes ISO/IEC 33000, risk management is covered by ISO 31000 and ISO/IEC 27005 focuses on IT-security risk management. Standards give guidance for process aspects of IT-security and Security by Design.

[2] This committee will also be able to fill gaps for standards which might be identified for example by ENISA or the industry.