Verband der TÜV e.V.

TÜV®

Date
22-Feb-18

VdTÜV position on the regulation proposal for a European "Cybersecurity Act" from 13 September 2017

Ten recommendations for a sound European "Cybersecurity Act":

1. VdTÜV welcomes that the requirements for the conformity assessment bodies comply with the "New Legislative Framework". In order to guarantee quality and confidence, only accredited third-party bodies shall be authorised for conformity assessment and certification. The interplay of independent conformity assessment, accreditation, notification, and national market surveillance provides effective and sustainable consumer protection.
2. The trustworthiness of a certificate is dependent on the assessment by an independent third-party body. Higher-risk products, services, processes, and systems must be subject to a mandatory assessment.
3. The certification must always merit the highest possible trust. It should be definitive, reliable, and transparent. A certification must always consider the risk of a product or service through depth and quality of the assessment. The higher the risk, the more comprehensive the assessment must be.
4. Since important functions are no longer components of the IoT product ("backend" systems), assessments must go beyond a limited product perspective.
5. The specification of responsibilities needs to be clarified. Who assesses and certifies, who notifies and who accredits must be clearly defined. To avoid conflicts of interests, the various actors may only be responsible for one single role at a time. Exceptions must be clearly defined and limited.
6. A label must be described specifically and consistently. It must provide a risk-adequate promise of security. Certification and awarding of labels require that an accredited third party carry out the assessment. The name of the responsible independent third party should be included on the label to promote trust. The underlying assessment criteria should be made publicly available in a transparent manner.
7. Given standards must offer a high level of trust in security. ENISA's new role must not cause existing standards to be undermined. Established high standards (e.g. ISO/IEC 15408) must continue to serve as the benchmark for a European security level.
8. The various interest groups must be closely involved with the development of the certification schemes due to their expertise and experience in these matters.

9. For assessment purposes, independent conformity assessment bodies require unrestricted access to the security-relevant data of the product or service (and their interfaces) under consideration of high data protection standards.
10. In addition to the regulation proposal, product and sector-specific requirements in respective “New Approach” regulations and directives must be reviewed and aligned with regard to information security. This requires a reassessment of risks. The aspect of the robustness of products and interoperability should be integrated into the definition of the general rules of product safety.

1. New risks arising from digitisation

Following the mechanisation, the electrification and the digitisation of industry, the widespread deployment of high-performance data networks in commerce initiated the fourth industrial revolution. Thus, the “Internet of Things” (IoT) is advancing into all areas of life and economy. New markets are emerging and the paradigms within the industry are being radically redefined. Real-time communication and the permanent exchange of large volumes of data enable new manufacturing and value creation processes.

A continuous series of new security incidents clearly demonstrates that the security of Internet-based products must be guaranteed across the entire product lifecycle and the entire ecosystem. Highly innovative products such as medical devices or connected vehicles, but also simple products such as electric kettles increasingly feature integrated software and use individual IP addresses. Due to updates and expanded functionality, which are no longer solely contained within the product, but also in the “backend” or the product network, the definition of products and the concept of product safety are changing.[1] Thus, the functional safety of a product is increasingly contingent on its information security.

The risk for the user of falling victim to cyber-attacks is increasing. Sensitive – and often personal – data can be manipulated, exposed, or destroyed. This applies in particular to critical infrastructure, i.e. neuralgic systems such as power and water supplies. Integrity,

[1] Cf. VdTÜV position: Regulatory improvement for safe and secure IoT products in Europe required, Berlin 2017 (https://www.vdtuev.de/dok_view?oid=680389)

confidentiality, availability, and the interplay of “safety”, “security”, and “privacy” of digital systems are essential requirements for the acceptance of digital social trends, making them the backbone of innovation and economic growth. It is paramount for innovations to be implemented securely to become progress.

As part of the 2017 cybersecurity strategy, the European Commission (EC) published a regulation proposal for the “EU Cybersecurity Agency” and the “Cybersecurity Act” in September 2017. VdTÜV welcomes the objective the EC is pursuing with this legislative initiative: strengthening trust in the security of products and ensuring a higher level of cybersecurity through a consistent framework for the certification of IoT products. A consistent certification framework can significantly contribute to ensuring that products and services are already secure before market entry and remain resilient throughout their entire lifecycle. Nevertheless, the present regulation proposal does not adequately take the long-term significance of secure internet-capable devices into account with regard to future societal developments and therefore requires substantial recalibration.

2. Guidelines for product regulation according to the “New Legislative Framework”

European legislation regulates a variety of products or sectors based on the “New Legislative Framework” (NLF, formerly, “New Approach”). This regulation model is the backbone of the European Single Market. It was developed to harmonise European product requirements in order to remove technical trade barriers in European and international markets.

The NLF limits product or sector legislation to the specification of essential requirements. These are described in detail in the directives and regulations, e.g., for lifts, pressure equipment, medical devices, or toys. Technical details are mandated by the EC and independently developed by the European standardisation bodies (CEN, CENELEC, or ETSI).

In order to place products on the European Single Market, they must be assessed for conformity with the existing and relevant requirements. The design of the conformity assessment process depends on the risk posed by the product. In the case of higher-risk products such as pacemakers or pressure equipment, the manufacturer must involve an independent third party (Notified Body). The independence of the body avoids conflicts of

interest and ensures highly reliable assessment results. The competence and independence of the conformity assessment body must be verified by the national accreditation body on an ongoing basis. This secures the necessary trust for the fulfilment of conformity assessment by private bodies.

For most products, the conformity assessment can be carried out by the manufacturer without the involvement of a third party. The identification of non-compliant products in the market falls on the national market surveillance authorities of the EU Member States.

- VdTÜV welcomes that the requirements for the conformity assessment bodies described in the regulation proposal for the "Cybersecurity Act" comply with the standard specifications of the NLF (Regulation 765/2008/EC). Annex I stipulates clear and strong requirements for the independence of conformity assessment bodies and provides for the free choice of bodies by the manufacturer. The same applies to the definitions used, which are in line with current EU legislation and internationally recognised norms. This ensures a clear and coherent legal framework for the benefit of all participating stakeholders.
- In order to provide convergence and comparability, only accredited conformity assessment and certification bodies may be responsible for the conformity assessment of IoT products. It is essential that these bodies meet a uniform quality level in the performance of their duties throughout Europe. The requirements and the quality level must be regularly checked by means of surveillance measures. This combination of independent conformity assessment, accreditation, and governmental market surveillance provides effective and sustainable user protection and reduces the burden on the state. This preventative approach is thus financed by the manufacturer, importer, or the retailers themselves.
- Additionally, it is important to ensure that the conformity assessment procedures meet the requirements of the dynamic and complex field of cybersecurity (see, for example, ISO/IEC 15408). This means they must be sufficiently flexible and readily adaptable to react to developments such as individual cyberthreat vectors. These procedures must also take into account the necessary manufacturer responsibility for updates.

- In addition to the regulation proposal, the product-specific security and health requirements in respective "New Approach" directives/regulations must be reviewed and adapted with regard to cybersecurity in the medium term. The currently existing regulatory gaps for IoT products have led to cybersecurity issues which are not, or not to an appropriate extent, a part of the obligatory conformity assessment.[2] Due to the expanded, dynamic functionality of IoT products, the issues of robustness (information security, data protection, and functional security) and interoperability must be integrated into the definition of the general concept of product safety (Directive 2001/95/EC).[3]

3. "Cybersecurity Act": Further specification and changes to the draft regulation

VdTÜV welcomes the effort to strengthen trust in the security of products through an overarching certification framework for IoT products. As long as all sector- and product-specific directives and regulations covered by the NLF are not comprehensively amended to include the aspect of information security, an overarching regulation can pave the way for the consistent implementation of specific security requirements. VdTÜV recommends the following further specifications and amendments:

a. Certification only on the basis of independent third-party assessment

The security of an IoT product is increasingly defined by the connectivity and data exchange within a digital ecosystem. This poses risks for the functionality, but also to external infrastructure, connected products, and services. As a result, risks and levels of criticality are shifting. A clear differentiation of the risk classes and a corresponding classification of IoT products must be the basis for the various voluntary and mandatory assessment procedures and the determination of necessary involvement of independent third parties. A multitude of security incidents in the past years has shown that the "duty of care" principle and sole reliance on manufacturer responsibility cannot guarantee a sufficiently comprehensive level of security.

---

[2] Cf. VdTÜV position: Information security of smart products in Europe, Berlin 2017 (https://www.vdtuev.de/dok_view?oid=680279)

[3] Cf. VdTÜV position: Regulatory improvement for safe and secure IoT products in Europe required, Berlin 2017 (https://www.vdtuev.de/dok_view?oid=680389)

- VdTÜV recommends that higher-risk products, services, processes, and systems be subject to obligatory assessment by independent third parties. A higher level of risk exists when an attack on the ICT product and service could compromise the confidentiality, integrity, availability, privacy, or other important objectives or could have implications for the health of users or third parties, the environment, privacy, or other important legal interests or critical infrastructures and their supporting systems or products (e.g. unauthorised interference with privacy or property). Therefore, the products and services listed as examples in the regulation proposal (including “connected cars”, industrial control systems [ICS], payment systems, or “smart grids”) must be subject to mandatory assessment and certification by independent third parties. The voluntary nature of certification in these product areas needs to be replaced by mandatory, independent third-party conformity assessment.
- The necessary trustworthiness and reliability of a certificate is mandatorily connected with the conformity assessment through an independent third party. Consequently, if a manufacturer seeks voluntary certification of a product, system, or service, an independent third-party assessment must be provided regardless of the degree of risk.
- The statement a certificate makes about the specifically defined cybersecurity properties of an IoT product must be definitive, reliable, and transparent. Regarding the depth and quality of an assessment, certification must always consider the risk posed by a product or service. This means, the higher the risk of the IoT product, the deeper and more comprehensive the assessment of the product or service must be. In the regulation proposal (Article 46), the “assurance levels” (basic, substantial, high) refer to the assumption that a “certificate [...] provides a limited degree of trust”[4]. They are therefore misleading without reference to the product-specific risk. Certificates must always merit the utmost trust and therefore, must

[4] Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), Article 46(2a)

be linked to the product-specific risk. Differences regarding the scope of a certificate must be derived from the underlying assessment criteria and processes.

b. Clear role and task distribution

The "framework" must ensure free competition between the independent conformity assessment bodies. Manufacturers must be able to independently select an accredited body on the market for the assessment and certification of their product or service. A clear separation of duties strengthens the necessary trust in the entire system and ensures fair, clear, and transparent competitive conditions on a 'level playing field' in Europe.

- The present regulation proposal requires clarification regarding the specification of responsibilities of national authorities and conformity assessment bodies. It must be explicitly defined who assesses and certifies, who notifies, and who accredits. To safeguard independence and avoid conflicts of interest and the concomitant negative impacts on quality and security levels, conformity assessment bodies, and approval and supervisory authorities should only have one role at a time. Therefore, neither approval and supervisory authorities nor accrediting and notifying bodies should function as certification bodies.
- The four-eyes principle and the separation of responsibilities must be observed for assessment and certification processes. The regulation proposal should be clarified accordingly.
- The role of the "national certification supervisory authorities" (Article 50) requires further specification. A strict separation of roles with regard to notification, accreditation, and certification should be ensured. The national supervisory authorities should be assigned the task of notifying the EC of the accredited conformity assessment bodies (Article 52(1)). Due to their function as notifying authorities, they should offer neither conformity assessments nor consulting services on a competitive basis. This serves to rule out any conflicts of interest.

c. Clearly defined exceptions

The regulation proposal provides that a certificate can only be issued by a public body (authority) in "duly justified cases" (see Article 48(4)).

- Upon appropriate consideration, "duly justified cases" can only arise where national security interests are directly affected. This includes, in particular, security interests that concern the core of the national polity or play a decisive role in defence of public safety – and therefore affect national interests in the narrow sense. Therefore, a significantly refined definition of the scope of application for governmental certification is required. From a regulatory point of view, comprehensive regulatory certification that goes beyond the core area of national security is an improper departure from the principles of European product regulation based on the NLF (Regulation 765/2008/EC).
- Furthermore, the definition of a "public body" referred to in Article 48(4) contradicts Article 48(3), by extending the scope of the term "public body", which suggests an authority, to privately organised and accredited conformity assessment bodies.

d. Consistent and transparent label

The regulation proposal (Article 47) stipulates that the conditions for the use of labels could be individually determined (per certification scheme for each product group). As a result, different certification schemes (or products, resp.) would require different conditions for the use of labels. In addition, this would lead to different requirements for the visual design of a label. Such a fragmented system would run contrary to the intention of creating transparency and guidance for the consumer.

- A consistent cybersecurity label should be specifically described in the regulation. Regarding their level of detail, the provisions set out for CE labelling in Regulation 765/2008/EC could be used as a reference. Depending on the respective product risk, the label must provide an adequate assurance of security and thus have uniform validity. The specific processes and conditions (assessment criteria) for

awarding a label could be regulated individually in the respective scheme, depending on risk and use case of the product or service.

- The name of the independent third party should be included on the label in order to strengthen trust, to ensure traceability and to facilitate legal action in the event of misuse (trademark law). In addition, users must be able to find a clear reference to the requirements and conformity assessment criteria (certification system) on the label. The underlying assessment criteria and processes should be publicly available in a summarised and easily understandable form.

e. Awarding labels only after independent third-party

The regulation proposal stipulates the voluntary nature of the label or certificate. At the same time, it is already set out in Recital 47 that the awarding of a label is to be carried out by an independent third party. Hence, if a manufacturer or service provider decides to apply for certification, the involvement of an accredited independent third party in the conformity assessment must be mandatory.

The certification of an IoT product or service requires that an accredited, independent third party – other than the product manufacturer or service provider – be included in the conformity assessment. The awarding (not the affixing) of a label by a manufacturer is thus excluded. Otherwise, this would undermine the trustworthiness of the entire certification framework.

f. Incorporating requirements in sector-specific regulations

The requirements of a certification scheme for specific products and services must, at least in the mid-term, be incorporated into the product and sector-specific requirements of the respective regulations and directives of the NLF – insofar as this is technically possible.

- The incorporation of specific cybersecurity requirements in product and sector-specific regulations and directives (in accordance with NLF) requires a reassessment of the risks posed by a product. Accordingly, it is necessary to carefully examine if an initial or more extensive mandatory involvement of an independent third

party is required. In the event of a complete implementation of the requirements, a label would provide no additional information about the trustworthiness of a product – thus rendering it obsolete.

- If important functionalities should no longer be a component of IoT products, but rather lie in the "backend system", the assessment must go beyond a limited product perspective. The possibilities of modern security architectures (e.g. secure encryption storage and distribution) must be sufficiently taken into account. Therefore, the existing conformity assessment procedures must be further developed.

g. Trust through high security levels

The new role of the ENISA must not cause existing standards and certifications process to be undermined ("race to the bottom") so that the lowest level of security becomes the European standard. The success of Industry 4.0 and digitisation depends on high standards that provide a high level of trust in security. Already established and recognised high national standards (such as ISO/IEC 15408) must serve as the benchmark for a European security level.

The assessment of the information security of a product or system cannot only be conducted by solely evaluating according to a static norm. Meaningful conformity assessment must take into account dynamic cyberattack vectors, which constantly change and expand.

h. Involvement of all relevant stakeholders

According to the regulation proposal, ENISA will take on a strategic role in a future certification framework. VdTÜV welcomes the possibility that, according to Article 44(2), all stakeholders should be "consulted" in the development of the certification system. However, it is necessary that stakeholders be closely involved in the development of certification schemes beyond mere consultation. The expertise and experience of all stakeholders (industry, independent third parties, and authorities) must be equally taken into account.

i. Data access for conformity assessment purposes

With regard to the cybersecurity and the data sovereignty of users (“privacy by design” and “privacy by default”), data-driven business models can contribute to enormous economic growth. The General Data Protection Regulation (GDPR) already provides the necessary European framework. However, VdTÜV observes a lack of a unified European market for data due to numerous other barriers. The result is that economic, social, and societal opportunities currently remain unrealised. Policymakers must create a legal framework within which data streams can move across borders and sectors. At the same time, data should be available in the best possible and most secure manner while allowing its usage for other purposes.

Independent conformity assessment bodies require unlimited access to the security-relevant control technology of the product or service (and their interfaces) for conformity assessment purposes. Moreover, manufacturers and service providers must inform independent conformity assessment bodies about changes to their IT components (e.g. software updates) so that the compliance of the system requirements can be further assessed and ensured. This goal can be achieved with minimal technical and economic effort.