Position paper

Requirements for coherent cybersecurity regulation

7th June 2019

Summary

The digitisation of all areas of our lives comes with advantages for consumers and opportunities for the economy. Widespread connectivity enables consumers to lead more comfortable lives. Time and cost savings increase economic productivity. To harness this potential, the digital industry wants to actively shape the latest chapter of the digital transformation.

While consumers and companies benefit from digitisation and improved networks, the growing number of networked devices (in particular IoT devices), the increasing complexity of digital systems, faulty software and the users' carelessness or inexperience with digital services can also be a target for cyber criminals. The prospect of financial gain coupled with a very low risk for the attacker — e.g. in the case of ransomware, where victims are blackmailed — makes cyber-attacks increasingly lucrative. This is why we are seeing a serious increase in attacks and an even greater threat potential, particularly in the area of security. Our goal should be to reduce the potential for attacks. Manufacturers and users, infrastructure operators, and criminal investigation authorities must work together to ensure the attack vectors remain as small as possible.

Regulation should be a framework within which companies across all industries consider IT security in product development, sufficiently check their products for security vulnerabilities, and provide security updates for reported security vulnerabilities. However, legislators must also ensure that regulations complement each other and that the companies subject to regulation be given reliability in terms of developing and marketing their products.

On the following pages, we examine existing regulations at the European level and provide food for thought for future developments in the field of IT cybersecurity legislation. As a basis for these considerations, we devised five demands, which represent the essential prerequisites for regulation in the area of cybersecurity.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Teresa Ritter
Head of Security Policy
T +49 30 27576-203
t.ritter@bitkom.org

Dr Katharina Eylers
Environmental Policy and Technical Regulation
T +49 30 27576-220
k.eylers@bitkom.org

Albrechtstraße 10
10117 Berlin

President
Achim Berg

CEO
Dr Bernhard Rohleder

1 Consistency of legal requirements

New regulation should always cover only those areas where there are regulatory gaps in order to avoid overlapping legislative requirements for the same product. Where regulatory areas overlap, consistency of all requirements and clarity of responsibilities (in particular those of supervisory authorities) must be ensured.

2 Equal requirements throughout the EU — safeguarding the single market

Cybersecurity requirements must be harmonised throughout the EU. They must not lead to fragmentation of the European Single Market, nor must there be differing approaches in individual countries. Ideally, European requirements are also compatible with global standards. This ensures and enhances a uniform digital single market and global competitiveness.

3 Requirements to be domain-specific and horizontally consistent

Sound cybersecurity requirements follow the same principles across all products but, within the individual product categories, describe specific requirements adapted and tailored to the specific area, also taking into account existing requirements or regulation in these domains. It must be ensured that security requirements are coherent and that cross-domain products (or products that can be used in more than one domain) are not subject to inconsistent requirements. In other words, it will be particularly important that different domain-specific requirements can fall back on a common basis taking into account the technical status quo.

4 Requirements based on risk and corresponding to intended use

Appropriate risk-based security requirements should be defined based on potential damage and their likelihood of occurrence in foreseeable use cases. The security requirements and the burden of implementing measures should be proportional to the risk. The security requirements should furthermore take into account appropriate requirements from domain-specific standardisation.

5 Agility and technical excellence of requirements through the use of European Standardisation Organisations (ESOs)

The digital industry has many years of experience with finding solutions and developing products which protect both their devices and their users. Within the national and European Standardisation Organisations, standards are developed and updated by experts from industry, business, and science in accordance with transparent and democratic procedures and taking into account the technological status quo. In order to strengthen industry competitiveness, harmonised European standards should be the preferred option. Doing so would reduce uncertainty for market participants, increase acceptance, increase the degree of direct technical feasibility, and ensure that requirements are up to date.

In the following, we would like to take a closer look at two important building blocks of European regulation — the Cybersecurity Act (CSA) and the New Legislative Framework (NLF) — in order to highlight their added value for increasing the level of cybersecurity. We then show how consistent interpretation of the individual regulations as well as between CSA and NLF is possible, based on the five principles mentioned above.

The Cybersecurity Act (CSA)

The Cybersecurity Act (CSA) was adopted in the beginning of 2019. The CSA establishes a legal framework which harmonises conformity assessment procedures (including certification) for products, services, and systems at European level. Requirements for cybersecurity are formulated in so-called conformity assessment schemes, against which devices, services, and processes can be voluntarily tested and, if necessary, certified. The declarations and certificates are valid in all European member states and substitute national schemes with the same criteria.

The Cybersecurity Act can, on the one hand, provide clarity for consumers and, on the other hand, greater consistency for pan-European companies. It is thus an important step towards greater security in the European Digital Single Market and greater confidence in the Internet of Things (IoT). Due to the rapidly increasing number of networked devices, there is a need for transparency and comparability, particularly in the consumer sector, in order to continue to sell secure products to the European market.

Where necessary, binding requirements can be established to accompany the voluntary conformity assessment, depending on the respective product criticality. To this end, proven concepts of product regulation should be used in the area of networked products, e.g. the New Legislative Framework (NLF).

The New Legislative Framework (NLF)

The New Legislative Framework (NLF), as the regulatory concept for technical harmonisation within the EU Single Market, allows flexibility of conformity assessment procedures and the involvement of stakeholders in standardisation. This system has proved to be successful and is worth preserving for the future, especially in view of rapidly evolving technologies and the digital transformation.

In many product areas (machinery, toys, electronic consumer goods), the NLF concept has contributed to improving the EU's competitiveness and securing its innovation potential

both through sectoral (e.g. Machinery Directive) and horizontal regulations (e.g. Electromagnetic Compatibility Directive). Where mandatory requirements are necessary, the NLF is therefore well placed to meet the challenges of cybersecurity regulation in the context of the digital transformation, and to create a regulatory basis for networked products in the EU Single Market.

In the NLF, only basic requirements are defined in EU directives (e.g. the products have to be safe to use and their operation should not interfere with other equipment), while specific technical issues are dealt with in mandated harmonised standards with the participation of industry in the European Standardisation Organisations (CEN-CENELEC, ETSI). All products to which these directives apply must comply with the essential requirements prescribed therein in order to be sold in the EU.

In numerous product directives, the European legislator stipulated a revision of the regulatory content of these directives when they were issued. This will lead to a revision in the coming years. The product-specific directives 2014/53/EU (Radio Equipment Directive) and 2006/42/EC (Machinery Directive) are currently being examined to determine whether cybersecurity should be included.

Due to the increasing relevance of cybersecurity for networked products, Bitkom welcomes the plan to strengthen the security of these products. In principle, Bitkom is of the opinion that the inclusion of cybersecurity requirements can supplement the protective measures included in the individual directives covered by the NLF. There is, however, a risk that when revising or supplementing existing guidelines of sector-specific products, no uniform requirements can be found. Instead, heterogeneous or even contradictory cybersecurity requirements may be the consequence for product categories that fall under several legal acts. This would be the case, in particular, if delegated acts were adopted which can only be formulated within the framework of the existing Directive, as is currently planned for the Radio Equipment Directive. The legislative process between the Commission, the European Parliament, and the Council must not lead to inconsistencies in the revised directives due to diverging interests; fragmentation must be avoided.

The interaction of NLF and CSA

As already indicated, the five principles mentioned above must be taken into account in when assessing and adapting regulations in the field of IT security. They must therefore be observed both in the aforementioned revision of the NLF and in the development of conformity assessment schemes within the scope of the CSA.

In addition, even if legal coherence within the two systems is achieved, consistency in the implementation of the NLF and the CSA and its future schemes must be continuously monitored. Conflicting requirements between the NLF and the CSA must be avoided, even if the certificates and procedures within the CSA are voluntary.

As already described, consistent cross-sector NLF regulation can help to foster cybersecurity while applying equally to all application areas. Notwithstanding, further cyber protection measures may be necessary for each sector, depending on the criticality of a given application and the probability of occurrence of a cybersecurity-related disruption. These requirements should be consistent with one another. Actively referencing the other regulation can be helpful in this regard.

Ultimately, a conceivable target could be to create one common framework for substantive legal requirements for product characteristics in line with the current level of development, so that corresponding regulation merely provides a regulatory and application framework. This would favour the development of consistent security requirements and, at the same time, open up scope for regulatory policy in order to create the necessary horizontal and, if necessary, vertical regulation.