Position Paper

on the EU Commission's proposal for a Cybersecurity Act

2017-December-20

Summary

In light of the growing global importance of cyberspace, the Internet as well as information technology systems, risks and threats to network and information security need to be minimised through intensified common European and international approaches. Bitkom, therefore, explicitly welcomes the European efforts to improve cybersecurity. The EU Commission's Cybersecurity Act could become an important step towards greater security in the European Digital Single Market and could lead to increased confidence in the Internet of Things (IoT).

A legal framework – harmonising procedures for the certification of IT infrastructures, products, services and systems at European level – would provide clarity for the consumer and might also have a positive effect on companies' risk management. One objective of the Cybersecurity Act should also be to increase legal assurance for pan-European companies. However, cybersecurity certification must not suggest that there is absolute security.

Getting it right presents a unique opportunity for equal competitive conditions and harmonizing national certification schemes. This, in turn, would ease access to the European market. Equal competitive conditions are essential for a functioning Digital Single Market and for the international competitiveness of European companies - strengthening their innovative capacity and for increasing the attractiveness of Europe as a location for business. Infrastructure operators, service providers and manufacturers should be equally required to develop their solutions (products, services, infrastructures) in a way that vulnerabilities can be avoided, identified or remedied at an early stage to reduce the risk of cyberattacks. The proposed legal framework can therefore only be effective and successful if it creates a harmonised European area for certification schemes in the field of IT security and addresses the entire value-added chain. The Industry has to play a decisive role in the design. Additionally, the implementation ought to be transparent and open. European and national standardisation organisations (DIN, CEN/CENELEC and ETSI) also should have a leading role in the establishment of standards. With their technical bodies and international collaboration agreements, these organisations are in an excellent position to carry out this crucial task.

Moreover, a purely European certification scheme is not appropriate due to the global

Federal Association
for Information Technology,
Telecommunications and
New Media

Teresa Ritter

P +49 30 27576-203
t.ritter@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

nature of the IT industry. Compatibility with international standards is absolutely essential for achieving an overarching security and harmonization structure. This also includes clear rules for the transition of existing certifications.

From Bitkom's point of view, an effective certification framework for IT infrastructure, products, services and systems at European level must be built on the following points:

1. The framework must take into account existing high international standards and agreements.

2. A distinction at least between products in the areas of consumer, business, critical infrastructure and high security, which could have an impact on national security, is needed.

3. An EU-wide harmonisation should not lead to a reduction of the already very high level of security in some member states and thus counteract the objective of the Cybersecurity Act.

4. The industry, national authorities and standardisation organisations must be involved in designing the system and setting subsequent standards.

5. Certification, as provided for in the proposal, should be voluntary in principle. During the upcoming legislative process it remains to be seen whether the certification framework achieves sufficient leverage effects for compliance within the standards and is able to ensure an adequate security level.

6. In order to further evaluate the present draft regulation, proposals are made for the design of the framework and additional certification methods, such as process-oriented schemes.

7. An extended role of ENISA must be designed in such a way that national sovereignty is not reduced.

Cybersecurity Certification

Bitkom welcomes the fact that the draft regulation aims at establishing a framework for an EU-wide cybersecurity certification scheme that is harmonised and internationally recognised. From Bitkom's point of view, seven key elements must be taken into account in the subsequent EU decision-making process:

1. Stronger referencing of existing international processes and standards:

A certification framework should not be understood as a prelude to introducing new standards. Rather, it should make recourse to existing norms and standards that are already widely accepted, such as the Common Criteria (as a standard) with CCRA or SOG-IS (as an agreement)-MRA. Already existing European cybersecurity certifications that are considered as best-practice should provide the basis for European harmonisation. Where a European approach promises a higher level of security than international approaches, it should be pursued globally within the framework of standardisation.

2. Differentiation according to the criticality of the different application scenarios:

Bitkom supports the three levels of assurance proposed in the draft (Article 46). In order to take into account the different application scenarios, the certification system should follow a risk-based approach that takes into account context and criticality and distinguishes between various cybersecurity risks. In this context, Bitkom calls for further clarification of the different levels of assurance and recommends a strict distinction based on individual risk assessments. This would enable, for example, to distinguish between consumer goods, industrial applications, and critical infrastructure software. The scalability of the certification system must be guaranteed in different areas and comply with the "moving target" in terms of security. In addition, clear regulations and guarantees are needed for the transition between existing certifications with regard to the further use of products.

With the increasing use of networked devices in the area of "Internet of Things", there is a need for additional action in the Digital Single Market to create adequate cybersecurity measures. If suitable security features are missing, IoT devices can in principle also serve as attack vectors and, due to their large sales volume in the member states, thus it is of great relevance for the EU. Particularly in this area, it is necessary to develop at least European, preferably international, standards that would increase the trustworthiness of IoT products. High-security applications, which could have an impact on national security (such as encryption products), must remain with the national remit of member states.

Bitkom advises against considerations such as those presented in recital 62 – the involvement of ENISA in the national cryptographic approval procedures of products. These issues are at the heart of the responsibility of national governments' work. In this context, it is absolutely necessary to protect national sovereignty.

3. Ensuring adequate security standards

Harmonisation across the EU should not lead to a reduction in high cybersecurity standards which have already been achieved and which are generally considered sensible. This would counteract the aim of this initiative to advance cybersecurity in Europe. In addition to relying on proven (inter)national standards and agreements, Bitkom considers the following points to be important:

Bitkom supports the creation of the European Cyber Security Certification Group (below the Group) as described in Article 53. However, Bitkom recommends that in order to ensure a high quality staffing of the group, the existing competence, experience and infrastructure in the field of cybersecurity in the respective member states should be taken into account. Failure to comply with these components may result in a decrease in the already high security standards in some EU countries.

There is a consensus that the "Security by Design" principle is especially essential for data security in the area of Internet of Things. For this reason, from Bitkom's point of view "Security by Design" must be the basic element of testing procedures within a European certification framework. The approach should be generic, as most security incidents result from the fact that the devices concerned do not even meet the most basic security requirements. In addition, such an approach could be flexibly adapted to changing technical conditions.

4. Greater participation of industry, national authorities and standardisation organisations

Voluntary business initiatives are one of the main pillars of improving IT security. Therefore, Bitkom demands that EU-wide certification schemes are going to be developed in cooperation with relevant stakeholders and with participation of industry. The proposal provides for a very limited industry involvement in the development and adoption of certification schemes. To ensure a high level of IT security, Bitkom asks that, besides the Commission and the Group, both industry as well as national and European standardisation organisations (DIN, CEN/CENELEC, ETSI) are going to be involved in the preparation of the standards. For example as part of "the Group". European and international standards – developed in a full consensus process – must form the basis for certification. In this way,

the process' openness would be guaranteed and at the same time standardisation would be made available in a quick and reliable way to ensure innovations in the field of cyber.

5. Voluntary certification

The draft regulation provides for voluntary certification (Article 48, paragraph 2). In addition to the design of certification – whether obligatory or not – the focus of the discussion should also be on the need for standard harmonisation. Mandatory regulation could be a barrier to market entry and hinder innovation. However, a level playing field is a prerequisite for the global competitiveness of European industry. In addition to achieving an adequate security level, a level playing field is therefore essential. This aspect should always be the starting point for the design of the entire system.

However, the draft regulation restricts the voluntary nature of certification to the extent that nothing else is provided for in EU law (Article 48, paragraph 2, second half-sentence). Bitkom understands that this regulation could be triggered in case voluntary certification does not lead to the desired goal, namely cybersecurity of ICT products and services and the strengthening of confidence in the Digital Single Market. The regulation therefore appears to be logical. At the same time, however, there is a risk that, in response to a failed voluntary certification, disproportionate measures could follow. The scheme opens the door to mandatory certification by conformity assessment bodies as defined in Article 51 on the basis of cybersecurity requirements, which were initially only intended for voluntary certification. Bitkom advises against this. Rather, the necessary design of individual standards and their compliance should focus on the respective leverage measures for achieving an adequate security level. These measures could In addition to minimum requirements for the solutions offered by infrastructure operators, service providers and equipment manufacturers, may include other measures which also appear to be appropriate for achieving the security objectives and which are less restrictive to the fundamental freedoms of the internal market. Bitkom calls for an intensive expert discussion on this subject in the further legislative process.

6. Framework design and complementary certification methods

The framework should be graded differently depending on sectors. For these different sectors, international standards should be chosen and national security should remain to be subject to national regulations. For the design of the respective security requirements, international standards should be selected, which contain the optimal requirements for the respective cybersecurity certification, depending on the application and target group.

Furthermore, if possible, certification should also be carried out from a process point-of-view, which makes demands on the manufacturers' development process. Product certification, which refers to a specific version and requires a partial re-testing after an update of the product, would be limited both in time and effort, especially for cloud-based applications. Bitkom therefore recommends that, in addition to product-focused schemes, process-oriented schemes should also be included as a supplement to a European certification framework, provided that such additions lead to a comparably high level of security and take into account the criticality of the respective application. To ensure a high level of security, a process certificate should state that the security-related development and operating processes meet high quality standards and are state of the art. Existing international standards that follow this approach (e. g. ISO 27034 for application security) should be used as the basis for a process-oriented schema. In order to ensure transparency and comparability, a further step must be taken to clearly define in which case and which type of scheme (product-focused or process-oriented) is to be used.

7. Extended role of ENISA

In principle, the envisaged expanded role of ENISA is to be welcomed. The upgrading of the agency is particularly important in the context of further harmonisation of cybersecurity measures throughout the EU's Digital Single Market. With a permanent mandate, it will be able to better coordinate cooperation between member states in the preparation and management of cross-border challenges to cybersecurity in the EU.

It is therefore a positive step if, in future, ENISA, which has been upgraded financially and in terms of personnel, is to promote operational coordination of the aforementioned co-operation, the development of defence capabilities and the exchange of information (info hub) – also in direct contact with companies. These measures would lead to a greater degree of harmonisation and legal certainty in the DSM.

According to Article 3 paragraph 3 of the proposal, the competences of the Member States with regard to public security remain unaffected. This is fully supported by Bitkom. The member states must maintain an effective degree of autonomy wherever national security is concerned. This should also apply to the area of the intended certification framework. Here the proposal is still too vague. In order for this argument to be used by the Member States in the interests of subsidiarity, clear rules must be laid down. However, a certain degree of autonomy must not mean that this will create regulatory gaps, which will ultimately lead to the creation of a fragmented cybersecurity system within the EU. In addition, it is important to note that the enhancement of ENISA's human resources focuses on quality – not quantity.

Conclusion

The steps formulated in the proposal can make a significant contribution to strengthening IT security in Europe, taking into account the above-mentioned points. However, the greatest concern should be not to concentrate solely on the European market, but to think internationally. This international dimension extends beyond the development and harmonisation of standards. As part of the B20 process, companies worldwide have called on the international community to develop standards for responsible government conduct in the field of cybercrime. An essential norm is the obligation of each state to stand firm against any kind of cybercrime emanating from its territory. The EU can and should become the driving force here.

In addition, Bitkom sees a lack in developing a broad approach that also focuses on consumers and users. For further legislative initiatives, Bitkom therefore recommends to think about strategies for increasing IT security, which allow the interaction of several instruments. Certification is always just a snapshot and ignores future technical developments and changes in the environment. For this reason, it is of particular importance to speed up and make certification procedures more manageable and to design them in such a way that, in addition to the high product quality they promote, they also pay more attention to the associated improvement of processes with regard to secure IT development within companies. At the same time, it must be clear that a mere increase in the number of certification bodies does not automatically lead to acceleration.

It also seems necessary to consider the "Cybersecurity Act" in the context of the new cybersecurity strategy "Resilience, Deterrence and Defence: Building strong cybersecurity in EU" presented by the EU Commission and the High Representative for Foreign and Security Policy in a joint communication. For the high-security sector in particular, the Cybersecurity Act should be placed in the context of the developing common security and defence policy, which is based on the strengths of the different member states.