COCIR contribution
to Public Consultation on the cybersecurity of digital products and ancillary services

Introduction

Rapid development of digital technologies drives economic growth across the world and offers great opportunities for economic growth and prosperity development, but the increasing cyber threats also pose major challenges for us. The digital security of our economies and societies is increasingly under pressure. The increasing connectivity also implies rise in cybercrime which is becoming more lucrative and therefore more attractive to malicious parties. Other factors such as the threat of state actors and a more unstable geopolitical world also contribute to the increased risks irrespective of the physical proximity to a source of threat.

To reap the benefits of digitization for the economy and the society, it is of great importance that European cyber resilience is strengthened. Cyber-secure digital products and services are an important element in securing resilience and sustainability of the EU member states.

Security is one of the aspects that needs to be addressed, next to interoperability, usability, and especially safety is at the core of the risk-based decision making. As most hardware products contain software products to be able to function, e.g., operating systems and middleware, any positive impact on the security of software products would directly improve the security of most hardware products.

Recommendations

1. Security requirements harmonization

Current agglomeration of security requirements in the RED/MDR/GPSD and many other legislations is a major concern. Also products might be used across multiple domains and be used by consumers and other end users, making adherence to a large set of partial overlapping and perhaps deviating or even conflicting requirements very complex. Therefore, we believe that Cyber Resilience Act should replace cybersecurity requirements under the RED and other broad legislations that have a broad scope and are not sector specific (e.g. MD/GPSD).

Horizontal common security requirements using harmonized standards under the NLF is the preferred approach. If it is essential, sector specific regulations may exempt, extend or increase the rigor of implementation and testing for sector specific security requirements.

2. Risk based approach to security and horizontal cybersecurity requirements

However, there is a significant difference in the level of cybersecurity from none to adequate depending on the sector and existing legislation.

COCIR members believe that a minimal "duty of care" mandatory cybersecurity requirements applying to everyone and everything is the best way forward. Also security should be risk based focused on the intended use and intended environment of use and as such the same level of rigor for security does not need to be applied to all products.

The EU will be able to promote its vision for high cybersecurity standards, including at international level, and strengthen the EU's global competitiveness only if all hardware and software used in the EU meet standardized cybersecurity requirements. Security should be grounded into a foundation of a risk-based approach, taking into consideration the intended use and the intended environment of use.

Mandatory requirements have some additional cost, but if horizontal approach is taken, it has a lower impact when there is a patchwork of requirements in different legislations.

3. Alighnment with established industry-specific and international standards

One key element for introducing voluntary certification schemes or mandatory horizontal requirements is the cost when these schemes/requirements deviate from the current state-of-the-art and established international standards. Many sectors have their own state-of-the-art like ICS/SCADA, automotive, medical, etc. which are based on established international standards (e.g., ISO 27000 series and the IEC 62443 series). Any horizontal schemes and requirements should be in support of those established (sector specific) international standards, not only to reduce cost for the manufacturer and support global market access, but also to make use of the expertise established in these international standards.

If member states would develop their own security requirements this would significantly increase cost and impact the single digital market. On the other hand, we have seen that member states are more willing to recognize international standards to demonstrate compliance to security requirements, in which case the impact is even positive for the single digital market and for international market access. A horizontal, NLF like approach that would recognize international standards would significantly align and improve cybersecurity across the board.

4. Definition of levels of security by the intended use and the operating environment

The risk categorization as currently used in the CSA might not be appropriate anymore as criminal organizations could be targeting a wide variety of ICT products, ICT services and ICT processes with state-of- the-art cyberattacks carried with significant skills and resources and therefor almost everything might need to be classified as high under the CSA.

Functional and non-functional requirements should be appropriate to the intended use and intended environment of use in relation to the reasonably foreseeable risk. As an example, two-factor authentication to be able to setup a Bluetooth connection between a hearing aid and a mobile phone is not only impractical but also has a huge negative impact on the usability of the product and has no direct perceived security advantages, there are other and better means to establish a secure connection.

Third party assessment/certification could be an appropriate tool to demonstrate compliance for high-risk hardware/software but should not be enforced in the CRA which has a horizontal approach.

5. Effective means to enhance confidence in cybersecurity

It is of the utmost importance that users can be confident that digital products, processes, and services they use are digitally secure. Yet one should always keep in mind that 100% safe does not exist. That's why we need more market incentives for the manufacturers, developers, distributors and importers of ICT products, services, and processes to take adequate cybersecurity measures. Coordinated Vulnerability Disclosure is an essential element to become aware of new vulnerabilities and as such directly linked to security by design. As such it should be supported by any economic operator, following clear, unified, and not excessive regulative guidance.

Security-by-design and by-default should be the guiding principle in the development of hardware and software. Recognition and use of international standards are a crucial element in the approach. The level of security must be appropriate to the intended use and the operating environment. To avoid inefficiencies and seamlessly align continuous needs for cybersecurity over the product lifetime with economic rationale, risk-based objectives instead of product/service requirements should be defined and followed.

Establishing security by design processes to be able to support a hardware/software product throughout its entire lifecycle is key and the most important element as hardware/software will most likely not remain secure over time. Also, security by default is important to ensure that less security savvy users are not exposed to unnecessary risks.

The secure use of products would benefit from organizational measures on the side of operators and users too. Therefore, COCIR also wants to point out the important role of operating procedures and users' qualification towards cybersecurity.

Providing updates should be supported on a risk basis only taking into consideration the intended use of the product (e.g., constrained devices). Replacement should be an alternative rather than enforcing update functionality in all products. If required there should be clear guidance on risk proportionality, timelines for mitigating and roles and responsibilities of all stake holders. E.g., an economic operator cannot be held responsible if the user does not apply the patch. Furthermore, a consideration of cost / effectiveness and a reasonable end of life after which any such obligations are no longer applicable.

We also believe that providing SBOM information does not improve security for consumers as the required knowledge is absent and as such there is no real cost/benefit. For other end users it might aid in their ability to do risk management and risk mitigations but as the design of the product and additional control measures are unknown, there will be a lot of false positive information especially when very granular information is provided, hence why SBOM information should be limited to a high level instead of full decomposition.

Conclusion

Software, by its very nature, needs to be updated regularly. The manufacturer/developer should be responsible for making updates available for vulnerabilities for a certain period to be determined in a European context. But a number of preconditions are important here, such as: risk-based, where the costs must be in proportion to the safety obtained, user responsibilities and a reasonable end of life after which such obligations no longer apply. It is also important that products that are placed on the market have the safest settings enabled by default.

Hardware manufacturers and software developers should be able to demonstrate that they comply with cybersecurity requirements. In principle, a hardware manufacturer's or software developer's own declaration of conformity gives sufficient confidence that the security requirements are met.

Third-party assessment may be an appropriate tool to demonstrate compliance with high-risk hardware/software. There must be European agreement on what is sufficient level of cybersecurity.

Possibly lex specialis, such as the MDR, should build on top of the CRA, with the necessary exceptions and extensions.