bitkom

Cyber Resilience Act

Bitkom Position Paper

At a glance

Cyber Resilience Act

Status quo

A high level of cyber resilience is a basic prerequisite for the smooth functioning of highly digitalized processes, networked products and services. However, companies, operators of critical infrastructures and private users today face a steady increase in cyber attacks. Manufacturers and operators must therefore protect all their products and software from an ever-expanding threat landscape - which is where the Cyber Resilience Act (CRA) comes into play. It will introduce cybersecurity requirements for all product categories based on the principles of the New Legislative Framework.

Bitkom evaluation

Bitkom generally welcomes the Commission's proposal to create a more efficient legal framework to improve cybersecurity. Nevertheless, we see some important aspects which should be optimized and clarified during the legislative process.

Most important

Scope

The European Commission's proposal takes into account the different phases of the lifecycle of a digital product and will contribute to a significant increase in the cyber resilience of the EU. From Bitkom's point of view though, the scope needs to be sharpened, especially with regards to encompassed products, Open Source, cloud services (Saas) and the CRA´s relationship with existing cyber security requirements and other regulations.

Essential requirements

Essential requirements must be non-discriminatory, proportionate and based on the intended use of the product. The CRA distinguishes between three types of products with digital elements: Products with digital elements, critical products with digital elements and highly critical products with digital elements. We welcome the approach of different classification levels. However, the classification of the products should not only be focused on the product itself but should account for their intended use and respective operational environment as well.

Implementation

After entry into force, stakeholders have 24 months to implement the new requirements. Since the scope of the law is very broad and covers physical products, the transition period is too short, especially considering the lack of standards, as well as the lack of expertise in standardization and implementation of the requirements in products. The adaptation period must be: 24 months for the documentation obligations, 36 months for criticality class II and 48 months for criticality class I. This approach would also consider the criticality of the products, the need to develop appropriate standards and accreditation of conformity assessment bodies.

97%

of companies in GER want policymakers to step up their efforts to promote EU-wide cooperation on cybersecurity

(Bitkom Research)

Bitkom Position

Due to the expansion of services in the digital sector and the increasing dependence on digital products, cyber risk has risen significantly. Even though security measures are constantly being adapted to these new challenges, criminal efforts are becoming more sophisticated and more digital. Cybersecurity is therefore a key prerequisite for a successful digital economy and society.

Bitkom therefore welcomes the EU Commission's draft for the Cyber Resilience Act (CRA) to create a more efficient legal framework for cybersecurity through the introduction of legislation on horizontal requirements.

The CRA will affect the ICT business in many respects e.g. as manufacturers, producers, operators and regarding vulnerability handling procedures. Generally, we support the approach taken by the European Commission to introduce a horizontal mandatory cybersecurity legislative act based on the principles of the New Legislative Framework (NLF). Such a horizontal approach is preferable to introducing even more cybersecurity requirements in different product-specific legal acts, as it avoids fragmentation of cybersecurity requirements. However, the current proposal contains requirements for products incl. software and obligations for manufacturers and other economic player but is unclear with regards to some of the details of these requirements.

In our view, the following aspects are some of the most important issues, which should be subject to further review and amended accordingly. As the CRA is of a complex nature and needs to be understood with reference to many other legislative instruments, further assessment will also be necessary during the upcoming legislative process and we would like to point out, that the following aspects are not exclusive and will be detailed later on.

Definitions

Numerous definitions are used to describe the products covered by the CRA (Article 3). To improve the comprehensibility of the scope and encompassed products (Article 2), it should be considered to include these definitions in Article 2 ("Scope") instead of Article 3 to describe the subject matter more precisely.

Furthermore, the definitions should be sharpened, those include, inter alia,

- significant cybersecurity risk (Article 3 No. 36), where the meaning of “significant” remains unclear[1]. The definition in Article 3 No. 35 describes the 'cybersecurity risk'. The definition (36) 'significant cybersecurity risk' should therefore clearly describe the circumstance "significant". The listed criteria, however, remain vague, e.g. high probability. It is questionable whether the definition fulfils its purpose. Since "cybersecurity risk" is already defined, there is no need to define "significant cybersecurity risk".

[1] The term is also referenced in the NIS2 Directive where Article 20 No. 11 provides that the Commission may adopt implementing acts further specifying the cases in which an incident shall be considered significant as referred to in paragraph 3.

- substantial modification (Article 3 No. 31) should be in line with the definition used in other EU Regulations, such as the proposed Machinery Regulation.[2]

- “limited attack surface” is used in Annex I No.1 (3)(h) but not defined in the Regulation at all. As the term needs clarification (especially “surface”) it should be included and described in Article 3 as well

- “regular tests” is used in Annex I No. 2 (3) but not defined in the Regulation at all. As the term “regular” needs clarification the term should be included and described in Article 3 as well

- “timely manner” is used in Annex I No. 2 (7) but not defined in the Regulation at all. As the term “timely” remains very vague the term should be included and described in Article 3 as well.

- “without delay” is used in various Articles, Recitals and in the Annex as well. This phrase remains unclear whereas “without undue delay” has a fixed legal meaning and should be used instead to avoid uncertainty.

- “known exploit” should be amended to „known exploits“ as the plural form is more accurate. Also, a definition for „known exploitable vulnerabilities“ is missing but referenced in the requirements of the Annex. We therefore propose to add that definition into the text of the CRA and use the existing terminology and definition of „vulnerabilities“ in Article 6 of the NIS2 Directive. Furthermore, as existing terminology refers to „known exploited“ vulnerabilities, the CRA should use that phrase as well instead of „exploitable“.

- For “importer” the existing definition according to Article 2(5) of Regulation (EU) No 765/2008 should be applied.

Essential Requirements

The European Commission's proposed list of essential requirements already addresses several important aspects that will increase Europe's cyber resilience. However, the proposal does not sufficiently address the intended use of a product with digital elements.

Scope (Article 2)

The proposed scope of the EU Commission refers to all "products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or

[2] We therefore propose the following new definition: substantial modification’ means a ~~change~~ modification to the product with digital elements following its placing on the market or putting into service, which is not foreseen by the manufacturer and affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed.

physical data connection to a device or network". With this, the Cyber Resilience Act is intended to ensure that all products with digital elements must meet basic cybersecurity requirements.

From Bitkom's point of view, this definition creates some confusion as to which products fall within the scope of application. Recital 9 creates uncertainty by excluding SaaS except for "remote data processing". Additionally, some critical products listed in the Annex can be delivered both in an on-prem or in in SaaS form. Indeed, cloud services, and as such SaaS, are already considered critical infrastructure and fully covered by the Network and Information Security (NIS) Directive 2.0.

Recital 10 excludes open source software that is not used in the course of a commercial activity but does not define the term or give detailes on how to assess the intended use and/or the determination of the intended use and/or a default category if no determination was done in advance. We suggest including that reference into Article 2 (Scope) of the CRA as well. In this context, it also needs to be clarified how the accountability requirements for open-source software components can be implemented in software. Lastly, it is also unclear what the relevance of the terms “indirect” and “logical” are.

Visible sign (Article 4)

Article 4(3) states that unfinished software which does not meet the essential requirements must be marked. It is already current practice to label such software as “Beta-Version”. The phrase "visible sign" is, however, not quite fitting for software products. We suggest amending the language here and include considerations on whether labelling the software encompasses the source code as well.

Criticality of products (Article 6 and Annex II)

In its proposal, the European Commission distinguishes between three types of products with digital elements: Products with Digital Elements, Critical Products with Digital Elements and Highly Critical Products with Digital Elements. We welcome this approach in general, as such a distinction follows the necessary risk-based approach. Different levels of assessments depending on the criticality of the products make sense. However, the assignment of products to these assessment procedures should be free of overlap and unambiguous, and the manufacturer should have a clear framework for action. Due to that we recommend an approach based on intended use, rather than the product category. The security level of products used in the area of critical infrastructure must not fall behind that of the infrastructure itself. The assessments must also be chosen accordingly. To reduce legal uncertainty given that the list cannot be considered exhaustive at all times, we urge the co-legislators to add the intended use of a product as the decisive characteristic for classification as (highly) critical. An approach based on critical infrastructure, industrial setting and consumers should be considered, also due to the economic impact on the pricing of products depending on the cybersecurity requirements a company has to implement. In this regard, the forthcoming Machinery Regulation, which deals with the impact of cybersecurity on life and limb, should also be kept in mind to prevent any overlap.

Further tightening will come from the inclusion of components in the scope and partly in Class III. Impracticable short transition periods will affect component manufacturers. It is to be feared that component suppliers will no longer be able/permitted to deliver at the end of the transition period. Even if the component manufacturer can then deliver a successor or new version of the component, this will come too late for the equipment manufacturer, because the replacement of components usually requires design changes, new tests, etc. There is also a risk that the Cyber Resilience Act in the EU will exacerbate supply chain issues for semiconductors. Device manufacturers still have big problems getting chips for their products on the world market. If chip manufacturers require additional approvals for their chips as a result of the Cyber Resilience Act, it is to be feared that they will supply EU customers on a lower priority basis or, in the meantime, not at all. Overall, the impact of the scope on often multi-level supply chains is highly critical.

Relation to other Union harmonization legislation (Art. 7-9, Recital 15)

Articles 7 to 9 describe the relation to other relevant Union harmonization legislation. We welcome the intention to avoid double and overlapping regulation, but we see the need for clarifications in the wording of Articles 7 to 9. Articles 7 to 9 are essential to all economic operators as well as market surveillance authorities. All stakeholders must have the same understanding and room for different interpretation should be avoided.

Recital 15 mentions the intention of the Commission to consider the repeal or amendment of Delegated Regulation (EU) 2022/30. For the sake of planning certainty, we would welcome the transfer of the substance of Recital 15 to the legal text as a new Article.

The proposed CRA is not the only EU Regulation addressing cybersecurity requirements for networked products. Other Union harmonization legislation such as RED 2014/53/EU already require conformity with cybersecurity requirements (by 1 August 2024), proposed texts for the new GPSR and Machinery Regulation also include security requirements.

It is essential for manufacturers - especially from the SME sector - to have clarity regarding the application of existing Union harmonization legislation. The relation among relevant EU harmonization legislation must be clearly described, easily understandable and most importantly avoid double regulation. The CRA should also introduce new specific requirements where none exist already and focus on filling gaps and harmonizing rules.

Obligation of manufacturers (Article 10)

We welcome the European Commission's core idea that manufacturers should only market products with digital elements that meet essential cybersecurity requirements, such as security by design and protection against unauthorized access. In addition, we welcome that all manufacturers are required to implement a structured process to

address vulnerabilities. To ensure that manufacturers of products with digital elements are informed of all known vulnerabilities, we call on European co-legislators to require government agencies - both supranational, national, and regional - to share their knowledge of vulnerabilities with the relevant manufacturer. Vulnerabilities, even if they can only be exploited by government entities, are a security risk for all and weaken Europe's cyber resilience. The Cyber Resilience Act can therefore only achieve its goal if both manufacturers and government agencies do their part.

The Cyber Resilience Act requires manufacturers of products with digital elements to address and mitigate vulnerabilities throughout the life of the product or for five years, whichever is shorter. The time frame for “life of a product” is not fixed and can be agreed upon by the contractual parties, taking criticality, quality, intended use, sustainability factors and other aspects into account as thus remaining flexible while accurate in relation to the specific product and its intended use. This is especially relevant since many products are already covered by other regulation (e.g. the Digital Content Directive Rules on Security Updates, other Certification Methods etc).

When considering changes after a product with digital elements was placed on the market, a product should not be considered becoming incompliant for the sole reason that a better product is subsequently placed on the market (cf. Article 6 (2) of Council Directive 85/374/EEC). There need to be differentiated and proportionate regulations in case a product becomes incompliant because of changes after it was placed on the market. The reaction of the manufacturer in such case should be commercially proportional, in particular after expiry of the warranty period. Depending on the individual case, the manufacturer should also be allowed to take actions to reasonably reduce risks, for example by warning customers, implementing controls or mitigations, or offering paid-for software/hardware upgrades.

We would also like to point out difficulties in the wording of the article. In Article 10 para 3 the term "clear justification" should be changed to "justification". The use of "clear" does not add any value, as a vague justification would not be recognized by the supervisory authorities.

Vulnerability & Incident Reporting (Article 11)

The Commission proposal requires manufacturers of products with digital elements to notify ENISA – as opposed to national competent authorities or CSIRTs - without delay and in any case within 24 hours of becoming aware of an actively exploited security vulnerability (as well as an any incident) having an impact on the security of in the product with digital elements (Article 11 point 1). The procedure appears to be inconsistent with the requirements set by the NIS2 directive and should therefore be aligned to ensure the notification process is efficient and contribute to overall product security. Therefore, in line with the NIS2 standard practice solely “significant incidents” should be reported.

In addition, Bitkom would like to see the reporting requirements of the CRA and NIS2 well aligned, as this would significantly reduce the administrative burden of the reporting obligations, avoid unnecessary layers of complexity in the reporting chains and make it even easier for the organization to know what to report and where and having legal certainty that they comply with the reporting obligation by reporting to

one authority (One Stop Notification). Therefore, it would be better to have the possibility to report to the competent national authority of the organization's headquarters rather than involving ENISA.

To ensure efficient reporting procedures, an efficient and secure digital reporting mechanism. In addition, competent authorities should have access to this information under the NIS 2 directive to ensure an efficient flow of communication (also, sharing the information with other national authorities could be a practical mechanism).

However, we are critical of the described approach that companies are only allowed a 24-hour window for such notifications. In order to analyze the situation and to write a corresponding report, this time window should be expanded to a maximum of 72h.

It also needs to be clarified when a product that is already on the market has undergone significant changes to the design and use of the product in order to fall under the notification requirement of the Cyber Resilience Act.

On a positive note, it should be mentioned here that both physical and electronic transmission of information and instructions is permitted (Article 11 point 10), as well as that EU conformity assessments can be accessed online (Article 11 point 11). We welcome a standardized API or web interface, which support efficient, automated reporting.

Hence, manufacturers should not only provide remedies for identified vulnerabilities but also provide their security updates on a regular basis, depending on the criticality of the product and its use. The time period within which updates are provided to close security vulnerabilities should be appropriate to the significance of the vulnerability and the criticality of the product, taking the use of the product into account. For example, major security updates of products used in critical infrastructure should be provided without culpable delay.

Rules and conditions for affixing the CE marking (Article 22)

Article 22(1) states that the CE marking in the case of software shall be affixed either on the Declaration of Conformity or on a website. The EU Declaration of Conformity is a mandatory document that either the manufacturer or the authorised representative must sign, declaring that the products comply with the EU requirements. By signing the declaration of conformity, one takes full responsibility for ensuring that one's product complies with the applicable EU legislation. The additional affixing of a CE mark therefore does not bring any additional benefit, on the contrary it is a duplication of the legal statement. The purpose of affixing the CE mark to the product is to signal conformity directly, switching to another place leads to confusion. Therefore, this requirement should be withdrawn.

In Article 11(6), the Commission may, by means of implementing acts, adopt technical specifications for pictograms or other signs relating to security of products with digital elements and mechanisms to promote their use, which shall be placed next to the CE marking in accordance with Article 11(3). Bitkom rejects the establishment of an additional mark for certain cybersecurity risks.

Demonstrating conformity (Article 24)

Bitkom welcomes the fact that the Commission proposal makes use of the conformity assessment procedures according to the NLF. It is seen as positive that here the conformity assessment procedures (Module A, Module B+C and Module H) reflect well the different risk levels of products with digital elements with regard to the scope of the directive. However, it would be welcome if the legislator would address the extent to which existing certifications or tests in accordance with internationally recognized standards can be used as proof of conformity for non-critical products and thus reduce additional expenses for companies.

In addition, the co-legislators should clarify whether only notified bodies in the internal market or also certified conformity assessment bodies (CAB) outside the internal market can perform the necessary conformity assessment for critical products with digital elements and whether it is possible for a single audit to cover multiple conformity assessments/certifications. This is of particular importance with regard to market access and competition in the EU. We want to highlight the need that enough notified bodies exist before the CRA enters into force because companies may need to have conformity assessments done in due time to ensure stable, uninterrupted production and delivery of goods and services.

Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk (Article 43)

Bitkom welcomes, the strengthening of market surveillance activities at national and European level, because effective market surveillance is an essential prerequisite for the effective and efficient implementation of the Cyber Resilience Act. However, it is important to ensure that these are implemented effectively and without overlap. This is the only way to ensure that companies that comply with the requirements are not put at a competitive disadvantage. It is essential that the market surveillance authorities of the 27 member states and ENISA ensure effective coordination among themselves. Accordingly, both the market surveillance bodies and ENISA must be provided with sufficient human and financial resources. The jurisdiction of the authorities of the Member States in cross-border cases appears unclear; multiple punishment based on the worldwide turnover needs to be excluded. The surveillance authorities should not be authorized to intervene without cause (e.g., Article 17).

Penalties (Article 53)

The Commission draft considers the introduction of monetary fines to ensure compliance with the defined cybersecurity requirements to be an appropriate measure. The proposed differentiation of these penalties according to corresponding misconduct seems justifiable from Bitkom's point of view.

However, we take a critical view of the fact that the basis for assessing the fine is based on the global annual turnover of the entire company. We believe that a better approach would be to base the assessment on the annual sales of the respective product.

Software Bill of Material (SBOM) (Annex I Section 2 Point 1)

SBOM as a stand-alone concept does not add much value. It needs to be part of an overall standards-based concept documenting details of the software but limited to essential information. For the latter, the German Federal Office for Information Security (BSI) is promoting the new concept of the Common Security Advisory Framework (CSAF), which is based on an open OASIS standard for security advisories. Bitkom points out that SBOMs are still in their infancy, and as such, have not yet achieved the required maturity level on how they should be implemented, shared and used as there is a lack on overall, standards-based concepts to implement SBOMs adequately). Therefore, it will be critical to ensure that regulators allow and support the private sector to coalesce on the standard-based concepts and formats that work best for given industries and organizations.

SBOMs should use standard-based and machine-readable formats integrated in an overall concept to support their uptake. The industry is already significantly investing in accelerating the maturation of SBOM standards and best practices. It is therefore crucial to encourage the private sector to continue developing new standard-based concepts and formats that work best for given industries and organizations, and for regulators to ensure close industry consultation when defining SBOMs requirements.

Secure software design, development, build, and distribution practices are well understood and defined in many industry standards and guidelines and have been for years. Software development organizations typically don't need to invent new approaches to solving security aspects but instead should focus on using and executing such well-established practices as described in the ISO/IEC 20243 standard, as well as the NIST Secure Software Development Framework (SSDF) for example, as the foundation for its security-by-design practices.

SBOMs are only useful if developers rely on them to identify and address vulnerabilities in dependency chains throughout the software development lifecycle rather than treat them merely as a reporting requirement.

Additionally, the CRA should specify that SBOM is only valuable when installing on-premises software and, thus, the SBOM requirements should only apply when a software product is shipped. SaaS (Software-as-a-Service) and cloud products should be required to attest that they manage their own supply chain and manage cybersecurity risk, but there is little value to requiring SaaS and cloud products to provide an SBOM. Indeed, these SaaS products operate via continuous delivery models, with weekly or even daily builds and deployments that would result in weekly or daily SBOM updates, and quickly make them outdated. While, at this stage, the CRA specifies that SaaS are not in scope of the Regulation (Recital 9), we have concerns that such exclusion is not sufficiently clear.

Timeline of the implementation of the Cyber Resilience Act

In order to increase the IT security of networked devices, the draft calls for a series of technical characteristics that regulated devices must fulfil (see Annex I). In addition, the device manufacturer is required to take further steps during product development and subsequent product support, including conducting a cybersecurity risk

assessment, performing due diligence when integrating third-party components, documenting relevant cybersecurity aspects, e.g. vulnerabilities that have become known, as well as implementing rules and procedures to disclose and address vulnerabilities (see Chapter 2, Article 10). We are of the opinion that these far-reaching obligations for device manufacturers with regards to product development and support can only be realistically implemented within the set 24-month period for those components that are fully under the control of the manufacturers. With regard to the device software, however, it is inevitable today that this is composed of in-house developments, purchased solutions from suppliers and open-source software, e.g. in the form of software libraries, applications or operating systems. It is precisely this dependence of device manufacturers on supplier software and open-source software that would make the correct and timely implementation of the Cyber Resilience Act close to impossible.

Given that the scope of the act is very broad the adaptation period is calculated too narrowly, especially, considering the lack of expertise of standardisation and the implementation of requirements in products. The adaptation period has to be prolonged. An option would be to base the adaptation timeline on the criticality of the product.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalization. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact
Simran Mann | Security Policy Officer | s.mann@bitkom.org
Rebekka Weiß, LL.M. | Head of Trust & Security | r.weiss@bitkom.org

Working Group
WG Security Policy