bitkom

Cyber Resilience Act

Bitkom Position Paper III

Cyber Resilience Act

Status quo

As Bitkom, we put forward our general comments on the Commission's proposal for the Cyber Resilience Act in two different position papers. As the discussions on the text are ongoing in Council and Parliament, we want to further elaborate on certain points to provide constructive additions during this process. In the following, we therefore give a more detailed assessment of certain articles and concepts within the Cyber Resilience Act that also picks up specific wording.

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. Building on our previous position paper we have compiled amendments based on a consensus approach within our diverse membership.

98%

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

Inhalt

1 Definitions (Article 3)

Numerous definitions are used to describe the products covered by the Cyber Resilience Act (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*

Article 3

Definitions

Amendment 1: Article 3 – paragraph 2

(2) 'remote data processing' means any data processing at a distance ~~for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;~~ that is enabled by a cloud service that the manufacturer of a product has designed and developed and is essential for achieving that product's primary function.

Amendment 2: Article 3 – paragraph 9 – new element

(9) 'incident' means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the product with digital elements offered by, or accessible via, network and information systems;

The current draft proposal lacks a definition of what constitutes an incident. This addition to the definitions aims to give guidance to the companies in which cases reporting procedures must be fulfilled.

Amendment 3: Article 3 – paragraph 18

(18) 'manufacturer' means any natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark~~, whether for payment or free of charge~~;

The amendment aims to align the definition with the New Legislative Framework, in particular the Market Surveillance Regulation (EU) 2019/1020. The aspect of 'whether for payment or free of charge' is also already covered in definition (23) ‚making available on the market '.

Amendment 4: Article 3 – paragraph 20

(20) ‘importer’ means any natural or legal person established ~~in the~~ within the Union who places ~~on the market~~ a product ~~with digital elements that bears the name or trademark of a natural or legal person established outside~~ from a third country on the Union market;

This amendment aims to align the definition for ‘importer’ to the existing definition according to the Market Surveillance Regulation (EU) 2019/1020.

Amendment 5: Article 3 – paragraph 21

(21) ‘distributor’ means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market ~~without affecting its properties~~;

This amendment aims to align the definition for ‘importer’ to the existing definition according to the Market Surveillance Regulation (EU) 2019/1020.

Amendment 6: Article 3 – paragraph 31

(31) ‘substantial modification’ means a change to the product with digital elements, exluding security and maintenance, following its placing on the market, 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;

The definition of substantial modification should be in line with the definition used in other EU Regulations, such as the proposed Machinery Regulation. Furthermore, it is of importance that regular security and maintenance updates are not considered a substantial modification since they do not impact the foreseen use and functionalities of the product.

Amendment 7: Article 3 – paragraph 33

(33) ‘national competent authority’ means any entity identified to perform the functions defined under Directive (EU) 2016/1148 or its recast;

We propose to align the reporting structures of the Cyber Resilience Act to the NIS Directive and have therefore added a definition referencing the national compentent authorities.

Amendment 8: Article 3 – paragraph 35

(35) ~~'cybersecurity risk' means risk as defined in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)];~~ 'vulnerability' means a weakness, susceptibility or flaw, as defined in NIS2 (art 6:15) and in scope with CSA (art 1), e.g., including ICT products, ICT services and ICT processes, that can be exploited by a cyber threat actor, while considerations for plausible exploitation has been given to provisions laid down in Article 5 and 10:10 of this regulation;

Cybersecurity risks are a term used for risks in relation to information security. However, vulnerabilities are the accurate term when referencing the IT security of hardware and software products.

Amendment 9: Article 3 – paragraph 39

(39) '~~actively~~ known exploited vulnerability' means a vulnerability for which reliable evidence exists that execution of malicious code was performed by an actor on a system without permission of the system owner. These known exploited vulnerabilities shall be subject to reporting requirements;

In technical terms it is more accurate to speak of 'known exploited vulnerability' rather than 'actively exploited vulnerabilities'. Known exploited vulnerabilities shall be subject to reporting requirements to the national competent authorities. However, in alignment to responsible disclosure they shall not be made publicly until a patch is implemented or made available.

Amendment 10: Article 3 – paragraph 40 – new element

(40) 'known exploitable vulnerabilities' means a vulnerability for which reliable evidence exists that execution of malicious code can be performed by an actor on a system without permission of the system owner. These vulnerabilities shall not be subject to reporting requirements;

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 Cyber Resilience Act and use the existing terminology and definition of 'vulnerabilities' of the NIS2 Directive 2022/2555. Furthermore, as existing terminology refers to 'known exploited vulnerabilities' the Cyber Resilience Act should use that phrase instead of 'exploitable'.

Amendment 11: Article 3 – paragraph 45

(41) ‘spare parts’ are ~~safety~~ components that are intended to replace identical components and are supplied by the manufacturer of the original product. The provision of spare parts shall not be regarded as a new placing on the market or a seperate placing on the market solely of the spare part.

Since not all spare parts are safety related components the word ‘safety’ should be deleted.

Furthermore, ‘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.

2 Scope (Recital 10 & Article 2)

From Bitkom's point of view, the scope of the Cyber Resilience Act is not sufficiently clear. Therefore, we urge the co-legislator to clarify the definitions listed earlier, keeping in mind the *lex generalis* nature of the Cyber Resilience Act. This applie in particular to Open source software and Software-as-a-Service.

Open source software is a major engineering tool for most industries and increasingly for the public sector. It lowers the barriers for entry to market, reduces overhead, and fosters competitiveness and competition. Therefore, it is essential to clearly exclude open source software from the scope of the Cyber Resilience Act. The current exclusion in Recital 10 lacks an accurate representation of the manifold realities of open source software.

It is fundamentally important to clearly differentiate between the joint software development within an open source software project (typically called “upstream” project) and the commercial use of the open source software in a product (typically called “downstream” use). The collaborative nature of upstream open source software development does not fit the concept of a manufacturer as no single responsible entity can be identified. Open source software is a common good. In contrast, downstream use of open source software is under the purview of a clearly identifiable manufacturer. As a result, it must be made clear that only the latter case is covered by the regulation.

Treating the inherently collaborative upstream open-source software under this regulation creates uncertainties and ambiguities with respect to responsibilities among the contributors to that software. This can result in a detrimental impact on

the open source software ecosystem, even negating the intended purpose of the Cyber Resilience Act by hampering contributions of security improvements.

Open source organizations facilitate the joint development of upstream open-source software by various contributors, but they do not act as individual manufacturers in the sense intended by the CRA. Therefore, projects hosted by such organizations as well as the organizations themselves should not be in scope of this regulation.

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 details 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 Cyber Resilience Act as well.

Amendment 12: Recital 10

In order not to hamper innovation or research, free and open source software (OSS) developed or supplied outside the course of a commercial activity should not be covered by this Regulation. T~~his is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.~~ Free and open source software (OSS) is defined as software, which is freely accessible, usable, modifiable, and redistributable. Free and open-source software is fundamentally based on collaborative development in a shared space (aka “upstream project”), thus placing it inherently outside of the realm of a single manufacturer. Therefore, the free and open-source software in this shared space (“upstream” project) is not covered by this Regulation. However, all free and open-source software can be used in the context of a commercial activity (aka “downstream” use). Commercial activities can be differentiated in profit-oriented activities, such as specific manufacturers that bundle FOSS to sell products and services and non-profit-oriented activities that usually foster the collaborative development of FOSS like the upstream projects themselves. This Regulation therefore applies only to such profit-oriented downstream use of free and open-source software under the purview of a specific manufacturer. The mere hosting or distribution of open-source software, participation in open-source projects, irrespective of whether a sponsorship or membership fee is paid, or technical support of a third person does neither make the person nor the OSS project a manufacturer nor qualifies as a commercial activity in the reading of this Regulation.

Amendment 13: Article 2(1)

Article 2

Scope

1. This Regulation applies to products with digital elements whose intended or ~~reasonably foreseeable use~~ forseen use as defined by the manufacturer includes a direct ~~or indirect logical or physical~~ data connection to a ~~device or~~ network.

In all cases it is reasonably foreseeable that a user operates a product in an environment that is neither foreseen nor intended for by the manufacturer. Using the current definition, 'intended or reasonably foreseeable', will force the manufacturer to design and develop the product always for the highest risk level. For example a temperature sensor intended to be used in a home environment could be used in a critical industrial environment. Would this scenario be 'reasonably foreseeable' and must be addressed by the manufacturer? From a cybersecurity and economic perspective, this would be neither reasonable nor appropriate. Lastly, this principle is also in alignment with industrial practices as well as the New Legislative Framework (NLF).

The current definition 'data connection to a device' would in practice mean that any product is covered if it communicates, independent of its cybersecurity risk. Covering indirect connections would in practice mean that any product is covered if it can potentially communicate. Instead due to proportionality considerations the focus should remain on cyber resilience. Products with digital elements that are intended to be connected to another device – but not intended to be connected to a network (the 'internet') should not be covered by the scope of the Cyber Resilience Act. Otherwise, all types of data connections between devices would be covered, including products which do not pose a cybersecurity risk.

Amendment 14: Article 2(2)

2. This Regulation does not apply to products with digital elements to which the following Union acts apply:

   (a) Regulation (EU) 2017/745;
   (b) Regulation (EU) 2017/746;
   (c) Regulation (EU) 2019/2144;
   (d) Regulation (EU) 2022/2555.

This amendment ensures that there is no regulatory overlap by excluding the NIS Directive 2022/2555 from its scope.

Amendment 15: Article 2(4)

4. This Regulation lays down specific rules and essential requirements with regard to cybersecurity for products with digital elements. Where other

Union legislation lays down requirements covering all or part of the risks covered by the essential requirements set out in Annex I of this Regulation, those requirements (or sectoral rules) in other Union legislation shall cease to apply.

~~The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where:~~

~~(a) such limitation or exclusion is consistent with the overall regulatory framework applying to those products; and~~

~~(b) the sectoral rules achieve the same level of protection as the one provided for by this Regulation.~~

~~The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend this Regulation specifying whether such limitation or exclusion is necessary, the concerned products and rules, as well as the scope of the limitation, if relevant.~~

Amendment 13: Article 2(6) – new element

6. This Regulation does not apply to

(a) free and open-source software in shared space (“upstream” project) is not covered by this Regulation. However, all free and open-source software can be used in the context of a commercial activity (aka “downstream” use). This Regulation therefore applies only to such commercial downstream use of free and open-source software under the purview of a specific manufacturer. The mere hosting of open-source software, participation in open-source projects, irrespective of whether or not a membership fee is paid, and technical support of a third person does neither make the person nor the OSS project a manufacturer nor qualifies as commercial use in the reading of this Regulation;

(b) ‘spare parts’ components for the repair of products with digital elements to replace identical parts integrated into products, provided that they are supplied solely for the repair of such products.

The provision of spare parts shall not be regarded as a new placing on the market or a separate placing on the market solely of the spare part. The Cyber Resilience Act should address the aspects of spare parts and define a realistic transitional period that allows the repair of products that have been placed on the market after the date of obligatory application of the regulation. This aspect should not be left out, especially considering the European commitment to sustainability.

This principle would also create alignment with the Blue Guide :

‘Such repair operations are often carried out by replacing a defective or worn item by a spare part, which is either identical, or at least similar, to the original part (for example modifications may have taken place due to technical progress, or discontinued production of the old part), by exchanging cards, components or sub-assemblies. If the original performance of a product is modified (within the intended use, range of performance and maintenance originally conceived at the design stage) because the spare-parts used for its repair perform better due to technical progress, this product is not to be considered as new according to Union harmonisation legislation.’ (The ‘Blue Guide’ on the implementation of EU product rules 2022, Repairs and modifications to products)

3 Criticality of products (Article 6)

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 primarily based on intended use environment. 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 essential requirements a company has to implement.

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 or 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 in particular. 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 classification as well as the scope on often multi-level supply chains is highly critical.

The following amendments aim to clarify the classification and create legal certainty for companies implementing the regulation.

Amendment 14: Article 6(1)

Critical products with digital elements

1. Products with digital elements that belong to a category which is listed in Annex III shall be considered a candidate to be critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products.

Amendment 15: Article 6(2)

2. The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list of categories of critical products with digital elements a new category or withdrawing an existing one from that list according to the scope under Article 6(2). When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the following criteria shall be taken into account:

~~(b)~~(a) the intended critical use in sensitive environments, including in industrial settings or by essential entities of the type referred to in the Annex [Annex I] to the Directive [Directive XXX/XXXX (NIS2)];

~~(a)~~(b) the cybersecurity-related primary functionality of the product with digital elements, and whether the product with digital elements has at least one of following attributes:

(i) it is designed to run with elevated privilege or manage privileges;

(ii) it has direct or privileged access to critical networking or computing resources;

(iii) it is designed to control access to sensitive data or operational technology;

(iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection.

(c) the intended use of performing critical or sensitive functions, such as processing of personal sensitive data;

(d) the potential extent of an adverse material impact, in particular in terms of its intensity and its ability to affect a plurality of persons;

(e) the extent to which the use of products with digital elements has already caused material ~~or non-material~~ loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse material impact.

The amendments of Article 6(2) aim to clarify the legal basis of the classification of products with digital elements by referencing its scope. Furthermore, the intended use environment of the product with digital elements is amended as the primary classifier.

Amendment 16: Article 6(3) & 6(5)

3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by 12 months since the entry into force of this Regulation]. Before adopting such delegated acts, the Commission shall carry out an impact assessment and shall carry out consultations.

5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. Before adopting such delegated acts, the Commission shall carry out an impact assessment and carry out consultations in accordance with Article 56 of Regulation (EU) 2019/881. When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is:

(a) used or relied upon by the essential entities of the type referred to in Annex [Annex I] to the Directive [Directive XXX/ XXXX (NIS2)] or will have potential future significance for the activities of these entities; or

(b) relevant for the resilience of the overall supply chain of products with digital elements against disruptive events.

These amendments aim to ensure to limit negative repurcussions on manufacturers and strenghten the democratic process by providing for an impact assessment and consultations.

4 Obligation of manufacturers (Article 10)

Amendment 17: Article 10(1)

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I. When implementing the relevant essential requirements set out in Annex I, the manufacturer shall take into account the state of the art, the costs and advantages/disadvantages of implementation of each individual measure and the intended use of the product with digital elements as well as the related risk of varying likelihood and severity.

This amendment aims to strengthen the risk-based approach of the Cyber Resilience Act in the implementation of the essential requirements.

Amendment 18: Article 10(4)

4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements. Manufacturers who exercised due care shall not be responsible for the fault of a third party under this Regulation.

This amendment shall protect manufacturers from liability for a fault of commited by a third party.

Amendment 19: Article 10(5) & 10(6)

5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity

aspects concerning the product with digital elements, including vulnerabilities they become aware of and any relevant information provided by third parties, and, where applicable, update the risk assessment of the product.

~~6.~~(a) When placing a consumer product with digital elements on the market, and for the ~~expected~~ estimated product lifetime or for a period of five years from the placing of the consumer product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

(b) When placing a non-consumer product with digital elements on the market, and for the manufacturer's estimated product lifetime or for a period of five years from the placing of the non-consumer product on the market, whichever is shorter, manufacturers will offer technical support (per agreements between a manufacturer and its customers), and support provided would be in accordance with the essential requirements set out in Section 2 of Annex I.

Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, consistent with ~~referred to in~~ Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.

This amendment aims to capture the complexities and differences of B2B products and consumer products in relation to the estimated product lifetime and associated technical support. In B2B environments each system/network is unique due to legacy, differences in the mix of generations of technology, software versions, and suppliers, hence technical support can be very resource intensive and should be defined prior through an agreement.

Amendment 20: Article 10(10)

10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible if the users may also be consumers. They shall allow for a secure installation, operation and use of the products with digital elements.

In the case of B2B products instructions might be more complex and technically challenging. Therefore, easily understandable language shall only be a requirement for consumer products since this does not reflect the realities of B2B products.

Amendment 21: Article 10(12)

12. From the placing on the market and for the estimated ~~expected~~ product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, or to implement other measures to reasonably reduce the relevant cyber risks such as additional safeguards, countermeasures or customer advisory, as appropriate.

The wording 'estimated product lifetime' is prefered to 'expected product lifetime' since the term estimate captures potential deviations in product lifetimes.

Amendment 22: Article 10(14)

~~14. A manufacturer that ceases its operations and, as a result, is not able to comply with the obligations laid down in this Regulation shall inform, before the cease of operation takes effect, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the concerned products with digital elements placed on the market.~~

Informing users is considered contra productive since it would also mean providing the public with information on future vulnerabilities. This would go against the principles of vulnerable disclosure by providing easily accessible information on vulnerable products to malicious entities and go against the intentions of the Cyber Resilience Act. Informing the market surveillance authorities before a company ceases its operations due to e.g., bankruptcy is not realistic.

We also suggest deleting the similar requirements for importers (Article 13(9)) and distributors (Article 14(6)).

5 Vulnerability & Incident Reporting (Article 11)

Amendment 23: Article 11(1) & 11(2)

Reporting obligations of manufacturers

1. The manufacturer shall, without undue delay ~~and in any event within 24 hours of becoming aware of it,~~ and when it has a reasonable belief that a critical or high vulnerability is present and exploitable in the product with digital elements, and after the manufacturer has issued clear remediation guidance, notify ~~to ENISA~~ to the national CSIRTs designated as coordinators pursuant to Article [Article 12(1) of Directive (EU) 2022/2555 ~~any actively exploited~~ known exploited vulnerability contained in the product with digital elements. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ~~ENISA~~ The CSIRT shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to ENISA ~~the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt~~ and inform the market surveillance authority about the notified vulnerability. Notification shall not subject the manufacturer to liability, and the manufacturer's report shall be protected from disclosure and cannot be used as evidence against the manufacturer.

2. The manufacturer shall, without undue delay and when it has a reasonable belief that a significant incident has occurred ~~in any event within 24 hours of becoming aware of it~~, notify to ~~ENISA~~ the national CSIRTs any incident having significant impact on the security of the product development, build and distribution environment of a product with digital elements already made available on the market. ~~ENISA~~ The national CSIRTs, designated as the single point of contact in accordance with Article [Article 12(1)] of Directive [Directive 2022/2555 (NIS2)] of the Member States shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to ENISA ~~the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned~~ and inform the market surveillance authority about the notified incidents. The significant incident notification shall include strictly necessary information to make the competent authority aware of the incident and allow the entity to seek assistance if requires ~~on the severity and impact of the incident~~ and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact. Notification shall not subject the manufacturer to liability and the report shall be protected from disclosure and cannot be used as evidence against the manufacturer.

In alignment with the NIS 2 the manufacturers should notify of known vulnerabilities to their respective national single point of contact as defined in the MS under the NIS 2 (i.e. CSIRTs). The national single points of contact should than transmit the notifications to ENISA, Furthermore, manufacturers should not be subject to liability when adhering to the requirements of the Cyber Resilience Act.

Amendment 24: Article 11(3) & 11(4)

3. ENISA shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established by Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity significant incidents and crises at an operational level.

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements, where appropriate and if likely to be adversely affected by ~~about~~ the significant incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

Significant incident should be in focus considering constraints in ressources as well. Furthemore, a flooding of notifications of the users can lead to indifference. Therefore, only significant incidents with potentially adverse impact should be communicated.

Amendment 25: Article 11(8)

8. The national CSIRTs and ENISA shall, in the case of becoming aware of vulnerabilities, inform manufacturers without undue delay of any significant incident having an impact on the security of the product with digital elements of the manufacturer.

To ensure security the national single points of contact and ENISA shall inform the manufacturers of any known exploitable vulnerabilities so that necessary action can be taken by the manufacturer.

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

Amendment 26: Article 22(1)

Rules and conditions for affixing the CE marking

1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to the accompanying documents or packaging.

Considering that the Cyber Resilience Act will also be regulation software products the option of affixing the CE marking to accompanying documents must also be provided.

7 Demonstrating conformity (Article 24)

Amendment 27: Article 24(3)

Conformity assessment procedures for products with digital elements

3. Where the product is a critical product with digital elements of class II as set out in Annex III, the manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements set out in Annex I by using one of the following procedures:

(a) the internal control procedure (based on module A) set out in Annex VI; or

(a) EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or

~~(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.~~

To allow manufacturers to merge management systems and avoid duplication of efforts internal control procedures based on module A should be allowed for.

8 Penalties (Article 53)

Amendment 28: Article 53(3) & 53(4)

Penalties

3. The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 10, except items 10 and 11, and 11 shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2.5 % of the its total ~~worldwide~~ annual turnover in the relevant Member States with the relevant product with digital elements in connection with the non-compliance for the preceding financial year, whichever is higher.

Items 10 and 11 of Article 10 should be covered under Article 47 of 'Formal non-compliance' since they refer to the accompanying documents of the product and not the product itself.

4. The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher. This shall only apply to non-compliance with 'essential requirements'.

Similarly, only non-compliance with essential requirements shall be subject to fines.

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

Amendment 29: Annex 1, (1.1)

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

~~(2)~~ Products with digital elements shall be delivered without any known ~~exploitable vulnerabilities~~ critical or high severity exploitable vulnerabilities;

Since vulnerabilities can not fully be ruled out it is essential to reframe the requirement by highlighting that no critical or high severity exploitable vulnerabilities should be present in the product after a risk assessment (see below). The definition of critical should follow an existing industry standard to ensure a harmonized approach, avoiding inconsistencies in compliance.

Amendment 30: Annex 1, (1.3)

(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) Products with digital elements shall be delivered after a risk assessment of their vulnerabilities

A risk-based approach calls for a targeted effort with the aim to rectify vulnerabilities that are likely to have a severe impact including considering environmental. This is essential, to ensure that stated objective of enhanced resilience in the Cyber Resilience Act is achieved by focusing valuable security resources and risk-management processes to remove critical and high severity vulnerabilities.

(b) be delivered with a secure by default configuration, or according to contractual terms for critical products with digital elements covered by ANNEX III;

While economic operators as defined in the Cyber Resilience Act are rightfully required to provide information to users according to ANNEX II, in the context of B2B and complex systems, manufacturers are not in the position to control security relevant decisions made by buyers of such products nor make decisions regarding the configuration of products to be integrated into their systems and networks. Furthermore, in these situations, each system/network is unique due to legacy, differences in the mix of generations of technology, software versions, and suppliers, hence it is impossible for a manufacturer to supply a product that is configured secure by default as this configuration will depend on the specificities of the unique system. This however does not take away from economic operators to provide information concerning secure configuration and operations.

(c) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(d) depending on the classification of data and the relevant intended use, protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encryption,

tokenization, compensating controls or other adequate protection of relevant data at rest or in transit by state of the art mechanisms;

(e) depending on the classification of data and the relevant intended use, protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(f) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(g) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(h) minimise their own negative impact on the availability of services provided by other devices or networks;

(i) be designed, developed and produced to limit attack surfaces, including external interfaces;

(j) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(k) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(l) ensure that vulnerabilities can be addressed through security updates, including, where applicable, separate from functionality updates and through automatic updates and the notification of available updates to users.

Full decoupling of security patches from regular upgrades is nearly impossible in the complex networks with high availability demands. Any upgrade must be tested on full-stack with full test-cycle without any adverse effects on availability. Therefore, it would be counterproductive to mandate decoupling of security fixes from functionality upgrades, as one reinforce the other. Therefore, shortening up of the product release cycle is more effective and secure in many environments,

Amendment 31: Annex 1, (2)

VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

(1) Identify and document known vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

Only vulnerabilities which are known by the manufacturer can be documented after identification.

(2) in relation to the risks posed to the products with digital elements, address and remediate critical and high known exploitable vulnerabilities without undue delay (allowing for testing and validating where applicable), including by providing security updates or document the reasons for not remediating the vulnerability;

As mentioned earlier critical and high known exploitable vulnerabilites should be in focus considering constraint in ressources as well. Furthemore the phrasing 'undue delay' allows for necessary testing and validation in sensitive environments to not disrupt essential services. Similarily, in certain B2B contexts vulnerabilities might not be possible to be remediated in due time due to the aforementioned reasons. For that it should be possible for businesses to take the informed decision to not remediate a vulnerability.

~~(3) apply effective and regular tests and reviews of the security of the product with digital elements;~~

This should be removed because the vulnerability handling process specified herein should be sufficient.

(4) once a security update has been made available, publically or according to industry best practice disclose information, to the extent necessary, about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

(h) information about such fixes and vulnerabilities is shared and disclosed in a controlled way respecting principles of "harm reduction" through responsible disclosure of vulnerabilities to the actors (operators of critical infrastructure in the telecom context) who can act to mitigate the vulnerability, and that it is not made public/widely available to avoid the risk of inadvertently informing potential attackers.

Both amendments refer to the principle of responsible disclosure to provide for a proportionate and risk-based approach for harm reduction.

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about known potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact

address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that known exploitable vulnerabilities are fixed or mitigated in a timely manner;

Similarily to the amendement above manufacturers can only take action on known vulnerabilities.

(7) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without undue delay or at a fair, transparent and non-discriminatory cost ~~and free of charge~~, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

While the effort of identifying and rectifying a security issue for which a security patch has been developed by a manufacturer, the dissemination of such a patch, free of charge is in gross contradiction with current industry practices of complex products/systems. A security patch typically requires significant efforts between different suppliers, integrators and operators of critical infrastructures, these activities require significant efforts and are typically planed in conjunctures with upgrades of functionality while ensuring that availability of such systems is not affected. To this end the Cyber Resilience Act should be proportionate and avoid a blanket imposition a free of charge dissemination model in markets where upgrades and patching of systems is complex, resource demanding and involves multiple stakeholders.

We therefore recommend that 'free of charge' is complemented with 'free of charge or at a fair, transparent and non-discriminatory cost' which has been used in regulation EU 2019/424 eco-design requirements for servers and data storage products. This would align with existing industry practice of security updates within complex products without risking fracturing the market.

10 Timeline of the implementation of the Cyber Resilience Act

Amendment 32: Article 57

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from [~~24 months~~ 24 months for the documentation obligations, 36 months for criticality class II and 48 months for criticality class I after the date of entry into force of this Regulation]. ~~However Article 11 shall apply from [12 months after the date of entry into force of this Regulation].~~

Considering the different types of products the Cyber Resilience Act will be regualting and the production cycles of these products a blanket transition period of 24 months can be considered unrealistic. Therefore, we propose a staggered approach to the different obligations under this regulation.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Simran Mann | Referentin Sicherheitspolitik & Informationssicherheit
T 030 27576-214 | s.mann@bitkom.org

Verantwortliches Bitkom-Gremium
AK Informationssicherheit