verbraucherzentrale
Bundesverband

RECOMMENDATIONS FOR A CONSUMER-FRIENDLY CYBER RESILIENCE ACT (CRA)

Recommendations of the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv) on the Cyber Resilience Act trilogue negotiations

10. August 2023

Impressum

Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

Team Digital and Media
digitales@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge hier und hier.

CONTENT

I. INTRODUCTION

The European Commission's (Commission) proposal for a Cyber Resilience Act (CRA) from September 2022 acknowledges the urgent need to improve the security of digital products on the European market. The Commission's proposal aims to strengthen consumer protection in the handling of connected devices. It therefore introduces mandatory cybersecurity requirements for products with digital elements covering computers, mobile devices, connected baby monitors or internet routers. In July, the European Parliament[1] (Parliament) and the Council of the European Union[2] (Council) adopted their positions to begin trilogy negotiations with the Commission.

The Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv) publishes recommendations for the following negotiations to highlight consumer interests and consider critical aspects and loopholes in the proposal and positions.

It is imperative that the CRA must establish a forward-looking and adequate level of protection. This includes sufficient basic requirements, appropriate timeframes for the disposal of security updates but also strict market surveillance and controls not dictated by industry logics. Therefore, vzbv suggests the following positions:

II. CORE RECOMMENDATIONS

1. CRITICAL PRODUCTS

- vzbv recommends adopting the Council's proposal of a clear and understandable risk methodology for future updates of the list (Art. 6 (1) (a)).
- vzbv supports the introduction of the European cybersecurity certification scheme by the Council and Parliament (Art. 24 (1)) established by EU legislation under the Cybersecurity Act (CSA)[3].
- vzbv welcomes the European Parliament's additions to the list of critical products in class 1 representing especially sensitive product categories for consumers (Annex III):
  - Smart home products (proposal by the European Parliament, Annex III, class I, 23 (a))

[1] Committee on Industry, Research and Energy: REPORT on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0253_EN.html#_section1, 09/08/2023

[2] Council of the European Union: Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 - Mandate for negotiations with the European Parliament, 2023, https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf, 04/08/2023

[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881, 11/08/2023

- Smart security devices (proposal by the European Parliament, Annex III, class I, 23 (b))
- Smart toys and products for children (proposal by the European Parliament, Annex III, class I, 23 (c))
- Wearables and health appliances (proposal by the European Parliament, Annex III, class I, 23 (d))

2. UPDATE OBLIGATIONS

- vzbv supports the Council's proposal of an open and unlimited time frame for security updates defined by the expected product lifetime which is aligned with consumer expectations and product related criteria (Art. 10 (6), recital 33 (a)).
- vzbv recommends the Council's (Art. 10 (10) (a)) and Parliament's (Art. 10 (6)) positions to disclose the end date for the provision of security patches to consumers at the time of purchase.
- vzbv supports the European Parliament's suggestion to separate functional and security updates (Annex I (1) (3) (a a)).
- vzbv recommends to introduce a transparent database on the average lifetime of product categories as suggested by the European Parliament (Art. 41 (9)) and the Council (art. 41 (11) (a)).

3. INFORMATION POLICIES

- vzbv welcomes the European Parliament's introduction of a point of single contact for users (Art. 11 (b)).
- vzbv supports the European Parliament's introduction of a complaining mechanism for consumers to the market surveillance authorities (Art. 41 (8) (a)).
- vzbv recommends to follow the European Commission's original proposal stipulating to report any incident with an impact on the security of a product (Art. 11 (2)) which is also maintained by the Council's General Approach.

4. COLLECTIVE ACTION

- vzbv welcomes the European Parliament's (Art. 54 (1, 2)) and Council's (Art. 54 (a, b)) proposal to include the CRA into the Representative Actions Directive (RAD).

5. APPLICATION TIMELINE

- vzbv suggests to follow the European Commission's original timeline of 24 months for the application of the requirements and 12 months for the application of Article 11 (Art. 57).

III. DETAILED EXAMINATION OF THE CORE RECOMMENDATIONS

1. RECOGNITION OF CRITICAL CONSUMER PRODUCTS WITH DIGITAL ELEMENTS

While the risk-based approach of the Commissions' proposal is reasonable for the introduction of a horizontal legislation, it unfortunately misjudges the criticality of consumer products. The division of products with digital elements into one basic category and two higher risk categories (class 1 and class 2) is the right approach to establish which products must undergo stricter certification processes. An examination of critical products by notified and independent bodies is necessary to avoid errors, conflicts of interests or inaccuracies. However, it is essential to identify critical products for consumers thoroughly and assess potential risks.

1.1 Art. 6: Categorisation of critical products

Unfortunately, the Commission and Parliament's proposals lack a comprehensible methodology for the categorisation of critical products leaving room for uncertainties and debate. The Council's approach introduces clear and understandable criteria essential for future updates of the list. Especially the reference to potential damages to "the health and safety of a large number of individuals" from the Council General Approach in Article 6 (1) (a) should support the inclusion of consumer products that are generally designed for the mass market and employed in numerous households.

1.2 Annex III: Critical products

The lack of consumer products in the Commission's proposal in either class is striking yet the Council has deleted even more products. Browsers or password managers are critical for internet and device security and must remain in the annex. The Parliament position makes essential additions to the list that Commission and Council must consider in the negotiations.

- Smart home products (Annex III, class I, 23 (a))

Smart Home products are working in a very sensitive environment, the private household and have the potential to affect multiple systems and products since they are usually connected to a broad network system. Vulnerabilities can compromise the fundamental rights to privacy and personal data and affect the safety and integrity of the user, for instance if the electricity control, a heating system or lights are manipulated.

- Smart security devices (Annex III, class I, 23 (b))

Among them are connected products fulfilling safety functions (for instance smart security systems, smart locks, alarms and cameras or smoke detectors). The case of a connected Abus door lock subject of an official warning of the German Federal Office for Information Security (BSI)[4] showed how the manufacturer knowingly neglected a severe vulnerability. Abus left its customers uninformed and vulnerable knowing that malicious actors could deactivate the lock. A third party certification and testing could have revealed the vulnerability before the distribution and hedged the product from potential criminal misuse.

- Smart toys and products for children (Annex III, class I, 23 (c))

Products designed for children must be secure for the contact with a particularly vulnerable target group, which is in need for special protection. Children devices include baby

[4] German Federal Office for Information Security (BSI): BSI-Warnung gemäß § 7 BSIG: Funk-Türschlossantrieb HomeTec Pro CFA3000 des Herstellers ABUS, 2022, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/2022/BSI_W-005-220810.pdf?__blob=publicationFile&v=13 , 01/11/2022

monitors, applications for education or connected toys. In malicious hands, these devices can endanger children as the example of the connected doll Kayla showed alarmingly[5].

- Wearables and health appliances (Annex III, class I, 23 (d))

Wearables such as fitness trackers or smart watches and other products offering health related functionalities collect and process particularly sensitive data. A data breach can grant delicate and highly private insights about users giving information about the location or habits. Furthermore, insufficient data security, manipulated information or wrong medical advice can eventually lead to long-term health problems.

STRICTER CERTIFICATION REQUIREMENTS FOR CRITICAL CONSUMER PRODUCTS

The Cyber Resilience Act must acknowledge critical consumer products bearing higher risks due to the area of application, the functions or the target group. The certification requirements for products employed in a private household, designed for health purposes or children as well as products with safety functions must not be solely based on a producer's self-assessment.

2. SUFFICIENT AND TARGETED SECURITY UPDATES FOR THE ENTIRE PRODUCT LIFETIME

The provision of security updates inevitably determines the lifetime of a digital product. If the manufacturer chooses to discontinue the service of detecting vulnerabilities and reacting to incidents, a secure usage of a product is no longer possible. When defining a mandatory timeframe for security updates it is decisive that the duration sufficiently reflects the general product lifetime. For connected products with manual functions this is often much longer than the service period of the manufacturer.

2.1 Art. 10 (6): Consideration of the expected product lifetime for security updates

The requirements in the CRA must reflect consumer expectations. Regardless of any digital functions, a user can reasonably expect to use a washing machine for up to ten years, as it is the case for most large appliances. Also in the light of sustainability, an early and artificial obsolescence would result in avoidable electronic waste and financially burden consumers forcing them to make new purchases.

vzbv supports the approach of the Council, introducing an open concept aligned with consumer anticipations of the expected product lifetime suiting the horizontal approach of the legislation. In contrast, the Commission's ceiling of security updates at five years maximum seems arbitrary excluding durable products and contradicting the Commission's Green Deal. Similarly, the Parliament's approach clearly reflects business before consumer interests. The introduction of the new concept of a "service period" does not clarify any legal uncertainties. A service period that is merely proportionate to the expected product lifetime will always lag behind the actual lifespan. The solution must be a sound definition of the expected lifetime taking into account consumer expectations not distorted by artificial obsolescence.

The Council (Art. 10 (10) (a)) and Parliament's (Art. 10 (6)) positions both require producers to disclose the end date for the provision of security patches to consumers at

[5] Forbrukerrådet: Connected toys violate European consumer law, 2016, https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/, 04/08/2023

the time of purchase. This is an important step towards transparency facilitating the purchasing decisions of consumers. The Parliament also adds the requirement to inform users actively about the end of security updates which greatly simplifies the information policy for consumers.

2.2 Annex I: separation of security and functional updates

In the same light, the separation of functional and security updates demanded by Parliament (annex I) must be considered. Manufacturers must label security updates as such and not use them to install other updates such as function-maintaining, function-changing updates or content updates. To simplify the handling of updates for consumers, the Commission should follow the Council and Parliament's demand for default automatic installation with opt-out options.

2.3 Art. 41: database on average lifetime of product categories

Lastly, the Parliament's (art. 41 (9)) to publish statistics about the average lifetime of products is the right approach to foster transparency and competition. Similarly the Council's proposal suggest to consider the publication of statistics about the lifetime of products (art. 41 (11) (a)). However, authorities should mandatorily disclose the information to streamline manufacturers' approaches and enhance consumer orientation.

> **USER-FRIENDLY UPDATE REQUIREMENTS**
> Security updates must be mandatory for the expected lifetime of a product and in line with consumer expectations. The expected lifetimes of different product categories must be publicly accessible and comparable. Manufacturers must install security updates automatically and separate them from functional updates.

3. EXTENDING INFORMATION TO CONSUMERS

It is essential that consumers are no longer kept at the end of the information chain and remain in the dark about incidents or vulnerabilities. When purchasing a product, the security features and risks must be transparent and understandable and manufacturers must provide channels to communicate with users and inform them about risks and countermeasures in case of an exploited vulnerability.

3.1 Art. 11: Single point of contact for users

vzbv supports the point of single contact for users suggested by the Parliament (art. 11 (b)) and also intended by the Council (annex II (2)). A competent and responsible contact point for security concerns and problems of consumers having the necessary expertise will be a valuable tool to facilitate the reporting of problems and enhance consumers' trust in digital products.

3.2 Art. 11, 41: Complaining and reporting mechanisms for consumers

Further, the Parliament's position makes valuable additions regarding a complaining mechanism for consumers to the market surveillance authorities (art. 41 (8) (a)). This is crucial to prevent a bottleneck where consumer can only report problems directly to the producer. It grants too much leeway to the manufacturers, if he itself can decide whether to forward consumer reports to the authorities. A reporting mechanism with the market surveillance authorities gives consumers the means to address issues at an independent and uninvolved institution and reduces dependencies towards the producer.

In contrast, the reporting mechanisms suggested by the Council counteract the transparent approach of the Parliament. In art. 11 (4), the Council deletes the requirement

for immediacy for manufacturers when reporting vulnerabilities and incidents to consumers. The Council gives the national Computer Emergency Response Teams (CSIRTs) the opportunity to inform users, but leaves it to the discretion of the CSIRT to decide about the information policy. While it is important not to disclose existing and yet unaddressed vulnerabilities for security reasons, it is at the same time not justifiable to leave consumers unknowing and vulnerable. Without disclosing further technical details, a warning with first and simple countermeasures must be mandatory. Article 11 (4) (b) of the Parliaments position can be a valuable addition granting ENISA, the CSIRTs and national authorities the rights to inform the public about an incident. However, this must be a mandatory requirement in case of hazard.

3.3 Art. 11: Reporting obligations of producers

The limitation of the Parliament regarding the reporting obligations to only “significant” incidents is adverse to a consumer friendly approach. While the Parliament introduces two criteria to determine a “significant” incident, the term creates legal uncertainties for consumers since it is not clear what constitutes a “considerable material or non-material damage” (art. 11 (2) (a) (b)). While is questionable whether access limitations to certain functions of a product, short-term failures or the manipulation or loss of certain data would be viewed as “considerable” these restrictions and damages can be detrimental for individual consumers.

> **ENSURING CONSUMER FRIENDLY INFORMATION POLICIES**
>
> Consumers must be admitted contact possibilities to address cybersecurity related issues. Likewise, the information of users about incidences and vulnerabilities must be mandatory to allow for swift individual protective measures and enhance trust.

4. ENABLING OF COLLECTIVE ACTION

The Cyber Resilience Act can only improve the protection of consumers if it equips them with sufficient means to enforce their rights. While the inclusion in the reporting systems and a complaint mechanism can raise awareness and facilitate problem solving, the Commission proposal lacked the tools to address unsolved and unaddressed vulnerabilities as well as uncooperative or non-compliant manufacturers.

Technical incidents and vulnerabilities are often too complex for individual consumers to understand. Additionally, they are often overwhelmed and intimidated by the prospect of long and resource intensive legal proceedings, so that the CRA must allow for representative actions of competent associations against manufacturers. The suggestion of the Parliament and the Council to include the CRA in the Representative Actions Directive (RAD)[6] is vital for consumers to have access to compensations in case of damages and must be adopted in the negotiations.

> **INCLUDING THE CRA IN THE REPRESENTATIVE ACTIONS DIRECTIVE**
>
> Consumer organisation must be able to enforce consumers’ rights by representative action. The CRA must follow the approach of the Parliament and Council and be added to Annex I of the European Directive on representative actions for the protection of the collective interests of consumers ((EU)2020/1828).

5. TIMELY APPLICATION OF BASIC REQUIREMENTS

[6] European Parliament: Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020L1828, 83/08/2023

The use of connected products and digital applications grows constantly and many digital products are by now a steady part of consumers' everyday life. Yet, the current legal gap leaves consumers at a constant risk making a swift application of the CRA imperative. Currently not a month goes by without news of new incidents and exploited vulnerabilities. Every postponement granting the industry time to adapt and develop standards will always entail new cases of harmed consumers from published email addresses to stolen personal details and passwords or banking information. However, a stolen identity for instance cannot simply be restored and leaked information will not under control of the consumer again.

Since both Parliament and Council aligned the CRA's reporting obligations for manufacturers to the requirements adopted in the NIS 2 Directive[7], producers will be able to implement an existing and proven system currently implemented by the member states. The application of article 11 should therefore not exceed 12 months.

Further, vzbv strongly recommends not postponing the Commission's timeline of 24 months for the application of the basic requirements. The CRA standardisation request will profit from the ongoing development of standards for the delegated act of the radio equipment directive (RED)[8] that can serve as a solid basis. The Commission just recently deferred application of the RED to 2025 granting CEN/CENELEC sufficient time to draft European standards for the cybersecurity of connected products and doing essential preparatory work for the CRA.[9]

NO POSTPONEMENT OF APPLICATION

The basic requirements of the CRA must apply as soon as possible. Taking into account preparatory standardization work as well as the national implementation of reporting systems for cybersecurity incidents, 24 months, respectively 12 months for the reporting requirements are sufficient.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1691488901977, 08/08/2023

[8] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.007.01.0006.01.ENG&toc=OJ%3AL%3A2022%3A007%3ATOC, 08/08/2023

[9] COMMISSION DELEGATED REGULATION (EU) /... amending Delegated Regulation (EU) 2022/30 as regards the date of application of the essential requirements for radio equipment and correcting that Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282023%294823&qid=1691488392470, 08/08/2023