SAFEGUARDING THE CYBERSECURITY OF CONNECTED PRODUCTS

Statement by the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv) on the European Commission's proposal for a regulation on cyber resilience (Cyber Resilience Act)

20. Dezember 2022

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digital and Media

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

CONTENT

I. SUMMARY

This statement provides the Federation of German Consumer Organisations' (Verbraucherzentrale Bundesverband - vzbv) feedback for the European Commission's proposal of the Cyber Resilience Act (CRA).[1] vzbv welcomes the European Commission's proposal introducing binding and harmonised rules on the cybersecurity of digital products. Today, connected products of the Internet of Things (IoT) and digital services often disregard cybersecurity, leaving problems and risks to European consumers unanswered.

The Cyber Resilience Act (CRA) is an important step to create a secure digital environment. However, the regulation must sharpen its focus on consumers and consider existing obstacles and disadvantages consumers face. A strong legal framework must be build on three crucial pillars:

- an extensive scope applying sufficient basic requirements for all connected products,
- a strong certification system with external checks for particularly risky products, and
- an effective market surveillance and enforcement policy.

CYBERSECURITY REQUIREMENTS FOR ALL CONNECTED PRODUCTS
It is crucial that all products adhere to basic cybersecurity principles to ensure a high level of security and resilience in a network. Adequate basic requirements covering the complete life cycle for all products are inevitable. The obligations must cover the confidentiality, integrity and availability of data, services and functions. Loopholes must not limit the commitment to cybersecurity. A strong encryption is essential and must be an obligatory part of the basic requirements of the CRA.

SUPPLY OF SECURITY UPDATES FOR THE LIFETIME OF A PRODUCT
vzbv supports the life cycle approach of the regulation. However, short update periods undermine the security of a product and are not sustainable. The CRA must require producers and providers to issue security updates at least for the expected lifetime of a product. Additionally, producers have to offer a competent and responsible single point of contact for security concerns and problems of consumers.

PROTECTION OF ESSENTIAL AND MANUAL FUNCTIONS
Producers must always secure the independent functioning of essential basic functions of a product. A disconnection from the system or internet must not limit or interrupt the operability of the original purpose of a smart product.

EXPANDING THE SCOPE TO CLOUD SERVICES
Every product in a network contributes to the security of the system as a whole and can likewise undermine it. The scope of the CRA must cover all products to achieve a secure digital environment for consumers. Services including cloud services such as Software-as-a-Service (SaaS) must be included to profit from indisputable cybersecurity requirements.

MAXIMUM PROTECTION FOR HIGH RISK CONSUMER PRODUCTS

[1] European Commission: 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, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454&qid=1663582330179; 12/12/22

The risk assessment must consider the integrity of consumers including risks for the physical and mental wellbeing, privacy and the private home. The impact of a possible incident on an individual consumer must not be underestimated vis à vis potential total damages.

Certain consumer IoT products are potentially more harmful. Products fulfilling safety or health functions such as wearables and smart security systems as well as products collecting sensitive private data including smart home products as well as all products designed for children require stricter certification and controls. The same applies to connected products using artificial intelligence. Third party certification must mitigate AI-related risks in connected products.

STRONG CONFORMITY ASSESSMENT AND INDEPENDENT CERTIFICATION
Certification and conformity assessments are essential to guarantee compliance with the basic cybersecurity requirements. The safest way to mitigate security risks is in-depth testing by independent third parties. External certification must be available and feasible for all producers and providers. Only then, the CRA can prevent conflicts of interest between manufacturers and consumers. Third party assessment must be mandatory for all high-risk products. Connected products from the highest risk level must further be subject to continuous external controls and examinations.

MARKET SURVEILLANCE WITH AND FOR CONSUMERS
Authorities and producers alone are not able to monitor the complete market of IoT products. The CRA must include civil society, science and research as well as consumers and consumer organisations itself to face emerging new threats and detect vulnerabilities. The CRA must avoid producers' incidence reports to function as main source of information for surveillance and enforcement. Reporting possibilities must be open to all actors granting research, civil society and consumer organisations the power to initiate a review by the responsible national market surveillance authorities.

24-HOUR NOTIFICATION OBLIGATION TO CONSUMERS
In case of a security incident, manufacturer must inform consumers within at least 24 hours to prevent possible consequential damage and avert harm. Producers must share technical and background information with affected consumers to raise liability claims.

REPRESENTATIVE ACTIONS DIRECTIVE AND PRIVATE ENFORCEMENT
The CRA must provide consumers with an easy way to claim compensation for damages and allow for redress. Therefore, the CRA must be added to the Representative Actions Directive to enforce cybersecurity requirements and protect the collective interests of consumers.

HEAVY FINES AND PENALTIES
To ensure compliant behaviour, the CRA must define proportionate fines and penalties. The CRA should align with the AIA and DSA and set maximum fines at six percent of the total worldwide annual turnover.

II. INTRODUCTION

On 15 September 2022, the European Commission presented a proposal for horizontal cybersecurity requirements for products with digital elements as part of Europe's Digital Decade.[2]

vzbv welcomes the proposal of the European Commission since the lack of cybersecurity in connected devices poses severe problems and obstacles to consumers. Until today, producers and providers understand users and consumers as the weakest link in a cybersecurity chain. However, it is not the alleged incompetence or ignorance of users that mitigates cybersecurity. On the contrary, consumers express great concerns about the security of digital products and feel their protection is inadequate in the area.[3] In 2022, more than two third of German consumers worry about the unencrypted exchange of information (79 percent), discontinued security patches (75 percent) or insecure authentication procedures (73 percent).[4] Consumers expect that connected devices and digital services are equipped with the latest and adequate cybersecurity technology.[5] However, they must trust in the goodwill of producers and have no choice but to accept the available information and policies.

The whole market suffers from great information asymmetries at the expense of the user. Producers often neglect the cybersecurity of their products. In Germany, three out of four consumers have already been victim to cybercrime.[6] Simultaneously, sciences, white hackers, or consumer organisations frequently reveal new security risks and vulnerabilities. Examples range from intelligent dolls[7], smart home devices[8] or radio door locks[9]. The present vulnerabilities allow attackers to spy on children, to access unencrypted data from private smart home systems and even allow unauthorised persons to physically access buildings, offices or flats. In many cases, the attacks do not require any outstanding technical knowledge or prerequisites; however, consumers have almost no way to protect themselves.

The CRA has the chance to become a powerful tool creating a market where only secure connected products are accepted and cybersecurity becomes self-evident in the European Union. In order to achieve this, the CRA must meet three basic requirements.

---

[2] European Commission: 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, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454&qid=1663582330179; 12/12/22

[3] vzbv: Verbraucherreport 2022. Die Lage der Verbraucher:innen, p. 11, 2022, https://www.vzbv.de/sites/default/files/2022-09/Verbraucherreport-2022_vzbv-forsa.pdf; 31/10/2022

[4] vzbv: Cybersicherheit bei vernetzten Geräten stärken, 2022, https://www.vzbv.de/pressemitteilungen/cybersicherheit-bei-vernetzten-geraeten-staerken, 31/10/2022

[5] vzbv: IT-Sicherheit bei Anschaffung, 2020, https://www.vzbv.de/multimedia/infografik-it-sicherheit-bei-anschaffung, 31/10/2022

[6] NordVPN: Studie Cybervorfälle, https://nordvpn.com/de/blog/nordvpn-studie-cybervorfaelle/, 31/10/2022

[7] Forbrukerrådet: Connected toys violate European consumer law, 2016, https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/, 31/10/2022

[8] Eurocomsumers: Hackable home project: Euroconsumers unveils worrying results for smart device owners, 2021, https://assets.ctfassets.net/iapmw8ie3ije/1YOk8JU1LogUJFn898wLH1/7302188d91713d1b007811c4e8343c84/Hackable_home_press_release.pdf, 31/10/2022

[9] German Federal Office for Information Security (BSI): BSI warnt vor dem Einsatz unsicherer Funk-Türschlösser der Marke ABUS, 2022, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220810_Warnung_ABUS.html, 31/10/2022

First, the scope must cover all digital products and services and apply sufficient minimum requirements without exception in order to avoid leaving some products as vulnerable entry point to a connected system. Second, especially critical consumer products such as wearables, smart home products or safety-related products must be subject to mandatory third party certifications and stricter controls to protect vulnerable areas that possibly endanger the integrity of consumers. Third, the interplay between a strong market surveillance and deterrent fines must ensure comprehensive compliance of producers and providers.

III. PROPOSALS FOR GREATER CONSUMER PROTECTION

1. CONSISTENCY WITH INTERACTING LEGISLATIVE PROPOSALS

The simultaneous negotiation of related proposals such as the revision of the General Product Safety Regulation[10], the revised Product Liability Directive (PLD)[11] as well as the Artificial Intelligence Liability Directive (AILD)[12] is an opportunity to create a congruent and strong legal framework for digital products.

Therefore, it is important that the CRA provides a solid cybersecurity-related basis and defines the material requirements for liability claims and law enforcement. Only the effective interlocking of the proposals can provide a complete protection of consumer so they can invoke obligations of producers and providers and assert their rights in case of non-compliance. The level of protection offered in the CRA determines the scope for actions of consumers and counteracts the market and information asymmetries currently disadvantaging consumers. In order to restore balance in the market of connected devices and digital services, the CRA must present an ambitious and extensive framework.

2. ESSENTIAL REQUIREMENTS AND OBLIGATIONS FOR PRODUCERS

vzbv supports the proposed broad scope applying the basic requirements to all products with digital elements. In this sense, it is not comprehensible that the CRA excludes Software-as-a-Service (SaaS) (recital 9). First, a separation of different services and solutions is not always distinctive and second, the exclusion contradicts the

[10] European Commission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0346&qid=1671189297625; 16/12/2022

[11] European Commission: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495&qid=1666941274500; 28/10/2022

[12] European Commission: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496&qid=1666941175220; 28/10/2022

horizontal approach of the legislation creating possible loopholes regarding a comprehensive and high level of consumer protection.

Up to now, policy makers' main focus has been to ensure a high level of security of industrial products, critical infrastructure or state security disregarding how important it is to include consumer products into a security chain to leave no weak spots. The connectivity of Internet of Things (IoT) products entails that all elements of a network influence its security. In a home office situation, this could mean that a vulnerable personal device can be exploited as an entry point into a business network. A smart but poorly secured vacuum cleaner can provide hackers access to a complete smart home system, a distributed denial of service attack (DDOS) can use private WIFI spots or devices for extensive requests until an attacked server collapses. The strongest network is only as secure as its weakest link.

A connected coffee maker might be considered as low risk taking into account the intended use and possible risk scenarios of the product itself. However, a vulnerable coffee maker can be an easy entry point to infiltrate a network. The network that a coffee maker connects with can vary from a household to a start-up, a hospital or a nuclear power plant. In this case, only a holistic analysis of the network can show what risk are at stake.

Adequate basic requirements for all products are inevitable. These prerequisites lay the basis for a common understanding of cybersecurity and bridge the gap between producers, politics and consumers. The former must consider cybersecurity for the entire life cycle of a connected device or a digital service. This is not limited to the development and production and must include a safe way to dispose or recycle products.

Often the view on cybersecurity and the demands placed on a product differ between producer and consumer. This leads to great uncertainties. In August 2022, the German Federal Office for Information Security (BSI) warned of a security vulnerability in a radio door lock.[13] The producer; ABUS, is the German market leader for safety products such as locks for bicycles or doors. The BSI indicated the risk level as high, considering an exploitation of the vulnerability to be realistic. This official warning is very rare and a tool the BSI only uses when the authority wants to prevent harm from consumers. However, the producer contested the authorities' assessment both in official communication and in direct customer dialog stating that ABUS would not see any significant risk.[14]

> **ARTICLE 2 CRA[15]: EXPANDING THE SCOPE TO CLOUD SERVICES**
>
> Taking into account the connectivity of IoT products it is crucial to build and maintain a secure system. The weakest link principle implies that the resilience of a system depends on the weakest component. Every product in a network contributes to the security of the system as a whole and can likewise undermine it. The scope of the CRA must not be limited to achieve a secure digital environment for consumers. The inclusion of consumer products and cloud services such as software-as-a-service in article 2 of the CRA is therefore essential.

[13] 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

[14] Stiftung Warentest: Abus lässt Betroffene im Stich, 2022, https://www.test.de/Sicherheitsluecke-Abus-laesst-Betroffene-im-Stich-5923244-0/, 01/11/2022

[15] All cited articles without legislative reference refer to the CRA

2.1 Article 5 CRA: Requirements for products with digital elements

vzbv welcomes the consistent application of cybersecurity requirements to all products with digital elements. In order to ensure a high level of security and resilience in a network it is crucial that all products adhere to basic cybersecurity principles.

It is appropriate to include the complete life cycle of a product covering the installation and maintenance of a product. Only a holistic approach applying *security by design* will protect consumers in their handling with the product and react to security related developments.

(1) Annex I Section 1 CRA: Essential cybersecurity requirements

Section 1 of Annex I covers fundamental cybersecurity goals such as the confidentiality, integrity and availability of data and information. This holistic approach to cybersecurity is crucial and ensures the best possible resilience of a system. In this regard, vzbv welcomes the commitment to *security by default* regulated in section 1 par. 3(a). Digital services and connected devices must protect consumers adequately and according to current standards from the very first use preventing for instance the assignment of an insecure or a standard password.

However, security settings and product properties should not only be secure during their period of use. The CRA follows the principle of *security by design* requiring products to guarantee cybersecurity in design, development and production (section 1 par. 1). The vzbv supports the life-cycle approach of the CRA which also includes testing and maintenance in the required vulnerability handling processes (section 2). Nevertheless, the operation of a product will always have an expiration date making it essential to make provisions for a secure disposal or recycling. While the CRA covers the design, development or production, and maintenance of the product (see recital 44) it does not address any precautionary measures for the end of the life-cycle. There must be an easy and secure possibility to delete all data from the memory of a product or service. Further, it must be possible to properly disconnect disposed devices from networks so that they no longer have access to critical services and information. Further, safeguarding important system information or migrating data to a new system or device must be possible in a secure manner. Only then the life-cycle of a product eventually ends.

Beyond that, a recycled product must ensure the safe disposal of all personal data of the last user and also meet the basic cybersecurity requirements securing the next life-cycle with a new owner. A recycled product must be equipped with the latest security updates and be subject to the vulnerability handling requirements.

> **PROVISIONS FOR DISPOSAL AND RECYCLING**
>
> A life-cycle approach must consider provisions for the secure destruction or recycling of a connected product or the discontinuation of a digital service. The CRA must add requirements for a possible disposal in Annex I, section 1 par. 3. The requirements should include a disposal strategy that ensures that producers and/or users can withdraw data and all elements securely and permanently when needed or requested.

If a product or a system has a vulnerability, one must assume that someone will exploit it. Hence, the legal framework must not weaken secure techniques and standards and the requirements must not leave loopholes for producers. Section 1 par. 3(c) determines that the confidentiality of data must be protected. The most powerful tool to

achieve the maximum confidentiality is end-to-end encryption. The protection of communication endpoints is key to privacy and security. However, the paragraph only lists encryption as one option. This gap contradicts a clear and strong commitment to encryption.

NO EXEMPTION FROM SECURE ENCRYPTION

End-to-end encryption must be mandatory. Rather than naming encryption as an example, section 1 par. 3(c) must underline the irrevocability of it to protect confidentiality.

Section 1 point 3 (k), of Annex I specifies the obligation to provide security updates. It is important that products notify users about security updates and install security updates automatically. However, it is important to distinguish different types of updates. While this applies to security patches, producers must offer functional updates separately. A functional update can add new functions or remove existing ones. It can lead to an increasing collection of personal data or restrict certain functionalities and must be optional.

SEPARATION OF SECURITY AND FUNCTIONAL UPDATES

Producers must disclose the intention and effect of an update in an easily understandable and accessible manner and indicate when an update alters, adds or removes functions of a product or service. Where possible, producers should separate functional updates from security patches. When a product installs updates automatically, they must not alter any functionalities.

vzbv underlines that section 1 point 3 (f) requires the protection of essential services. This must however, not only include digital functions, but also apply to all manual functions and services. Particularly white goods and smart home products must not lose their original function because of a cyber-incident. A smart refrigerator must always be able to maintain the temperature and a smart washing machine must be designed so that the basic functionality of the washing programs are always available independent of the connectivity and digital functions.

This is especially critical when it comes to products with safety functions. The physical impact of an outage became apparent when Facebook experienced a worldwide incident. Not only were Facebook and its apps such as Instagram or WhatsApp inaccessible for several hours, but also employees were not able to access offices or conference rooms that were connected to the system.[16]

[16] Business Insider, Facebook employees reportedly couldn't access conference rooms and other systems amid of widespread outage, 2021, https://www.businessinsider.com/facebook-employees-no-access-conference-rooms-because-of-outage-2021-10, 09/12/2022.

New York Times, Gone in Minutes, Out for Hours: Outage Shakes Facebook, 2021, https://www.nytimes.com/2021/10/04/technology/facebook-down.html, 09/12/2022.

PROTECTION OF ESSENTIAL AND MANUAL FUNCTIONS

Producers must always ensure the independent functioning of essential basic functions of a product. A disconnection from the system or internet must not limit or interrupt the functionality of the smart product for its original purpose.

2.2 Article 10 paragraph 6 CRA: Security updates

vzbv welcomes the lifecycle approach of the CRA defined in the vulnerability handling processes sustaining cybersecurity also beyond the development and production phase (Annex I, section II). The role of security updates to ensure the security of connected devices during their lifetime cannot be overestimated. The regular supply of security updates is therefore of great interest to consumers. The discontinuation of security patches can lead to the complete uselessness of a product with digital elements. Even more: the continued use of an insecure product, no longer supplied with security updates, can cause significant consequential harm to consumers.

To limit the obligation to provide security updates to a maximum of five years is therefore not comprehensible and contradicts the life-cycle approach of the regulation. It also conflicts with sustainability requirements as it introduces an expiry date ignorant of consumer needs and habits. Recent analysis show that the average usage and replacement cycles for digital products such as smart phones are increasing. Currently, the average European consumer uses their smartphone for more than three years.[17] At the same time, many consumers decide not to purchase the newest version of a product to save money. This saving decision must be possible without forfeits in cybersecurity.

Other products such as smart home appliances have a much longer lifespan. On average, households use a washing machine for almost 15 years; a notebook is used for more than five years.[18] A long lifetime and usage period is particularly desirable as it not only saves the money for new purchases but also effectively helps to reduce resource consumption and emissions.[19] The CRA must therefore apply sustainability standards and enable the longest possible lifecycle of a product.

APPLICATION OF SUSTAINABLE UPDATE FRAMEWORKS

The CRA should acknowledge the need for a sustainable use of connected consumer products and must not limit the possible service period. Instead, it must take into account the average life cycle of the product type as well as the period of distribution on the market.

2.3 Annex II CRA: Information and instructions to the user

vzbv welcomes that producers have to offer a point of contact to users. Annex II point 2 obliges them to provide information regarding vulnerabilities. Further consumers should be able to report problems and incidents at the point of contact. However, it is essential to clarify how this point of contact is designed. A reference to the general customer support or a website form for instance is not sufficient to process cybersecurity issues.

---

[17] Euler Hermes: Can 5G reignite the smartphone industry?, 2022, https://www.allianz-trade.com/content/dam/onemarketing/aztrade/allianz-trade_com/en_gl/erd/publications/the-watch/2022_02_035G.pdf, 01/11/2022

[18] Greenpeace Schweiz: Ökologische Auswirkung einer längeren Nutzungsdauer von Konsumprodukten in der Schweiz, 2022, https://www.greenpeace.ch/static/planet4-switzerland-stateless/2022/03/70b24402-o%CC%88kologische-auswirkung-nutzungsdauer.pdf, p. 24-25, 01/11/2022

[19] ibid.

The point of contact must therefore be sufficiently equipped to provide information and advice as well as to analyse and handle vulnerability reports.

SINGLE POINT OF CONTACT FOR CYBERSECURITY

Producers must provide a "single point of contact" that is exclusively responsible for cybersecurity of the product and has the necessary expertise and authority within the company. The single point of contact established in the Digital Service Act (DSA) requiring platforms to offer a point of direct communication can act as a blueprint.

3. RISK CATEGORISATION OF PRODUCTS

Even though all connected products in a network contribute to the security of the whole system, it is out of question that some products are more risky due to their features or their intended use.

A risk assessment must take into account the severity of the harm. However, when it comes to data and figures, consumers are strongly disadvantaged. Currently information on the security features of an IoT product are usually not available and if the producer presents information it is not verifiable for users. This information asymmetry makes it impossible for consumers to evaluate the security of a product or react to vulnerabilities.

In case of a security incident, users are often informed late and insufficiently. Due to the technological complexity of the devices and services, it is not possible for consumers to understand whether a reported vulnerability has been exploited on their product and to identify the possible consequences. However, the enormous number of data breaches in the last years shows the extent of the problem. After data breaches of numerous platforms and providers, billions of user accounts were openly available on the internet. The information included email addresses, log-in credentials, credit card information or health and personal data.[20] However, the data leak is not the end of story: German consumer organisations regularly report cases of identity theft resulting from data breaches.

The reports range from unauthorised subscriptions to video streaming services or dating portals to the unauthorised creation of chargeable mail accounts to unauthorised orders of goods via shopping platforms.[21] The consequences often entail financial harm and longstanding, exhausting legal disputes and uncertainties for the affected consumer.[22]

CONSIDERATION OF CONSUMER HAZARDS IN RISK ASSESSMENT

A risk assessment must always consider the risk to the integrity of consumers. The physical and mental wellbeing, the financial situation as well as the respect for privacy and the private home are especially sensitive. An incident that threatens or harms any of these areas has to be considered as particularly critical and severe for an individual user. An assessment must always take into account the potential risks

[20] Information is beautiful: World's Biggest Data Breaches & Hacks, 2022, https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/; 24/10/2022

[21] vzbv: Identitätsdiebstahl in der digitalen Welt weit verbreitet, 2017, https://www.vzbv.de/pressemitteilungen/identitaetsdiebstahl-der-digitalen-welt-weit-verbreitet; 24/10/2022

[22] vzbv: Beschwerden zu digitalen Zahlungsdiensten erneut gestiegen, 2022, https://www.vzbv.de/meldungen/beschwerden-zu-digitalen-zahlungsdiensten-erneut-gestiegen; 24/10/2022

for the private and family life, home and communications and financial resources of consumers.[23]

3.1 Article 6 CRA: Critical products with digital elements

An extensive basis for the assessment of the riskiness of products with digital elements is essential. The CRA must provide a safety net for particularly risky products that does not only depend on the producer or provider and includes external checks. vzbv welcomes the approach of a risk assessment taking into account factors such as the sensitivity of the intended use, possible adverse effects or security functions of a product. However, the criteria exclude important risks to consumers.

(1) Article 6 paragraph 2 (b) CRA: Critical products with digital elements

Article 6 par. 2 (b) considers the use of a product with digital elements in sensitive environments. However, the paragraph mainly focuses on industrial settings. This omits the sensitivity of the private area as well as health and safety purposes. Smart devices are particularly critical if they collect personal or sensitive data or if users intend them to fulfil health, safety or essential services. Producers must particularly protect products such as wearables collecting health data and connected health appliances. The risks regarding health or security devices are particularly severe since the manipulation of the function of a device or errors in data can directly compromise the physical wellbeing or integrity of a person. A wrong number of steps issued by a fitness tracker might be less critical; however, if a device gives manipulated oxygen saturation or heart rates, it can severely threaten the wellbeing of users.

Another area is the safety domain including all products fulfilling safety functions such as smart security alarms, smoke detectors or carbon monoxide alarms, door locks or security cameras. A smart lock or alarm system must be secure against brute force attacks allowing unauthorised persons to enter a building or an apartment. The case of the vulnerable radio door lock from ABUS underlines how the self-assessment and interpretation of a producer can differ from an external or official evaluation. Months after the warning through the BSI, ABUS still refuses to help affected consumers ignoring the vulnerability. ABUS does not exchange the product and cannot offer an update since the vulnerability is hardware based. An external certification could have revealed the vulnerability before the distribution of the product and prevented the situation.

PROTECTION OF PRIVATE CONTEXT AND HEALTH AND SAFETY SERVICES

The definition of high-risk products must take into account all sensitive areas for consumers and include them in Article 6 par. 2 (b).This includes products designed to fulfil safety functions as well as health services or devices installed in the private environment, collecting sensitive data.

(2) Article 6 paragraph 2 (d) CRA: Critical products with digital elements

Article 6 par. 2 (d) assesses the potential intensity of an incident considering how many persons an exploit could affect. However, this approach can create an inclined situation where widely used products are potentially safer than products from less known manufacturer. This would especially harm customers of products from Start-ups or smaller businesses, which would often not have the resources to offer products with an external

[23] European Union: CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, 2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF; 24/10/2022

security evaluation. In addition, the definition of a “plurality of persons” remains unspecified leaving room for interpretation and excluding important products.

INCLUSION OF PRODUCTS OF SMALLER PRODUCERS IN RISK ASSESSMENT

The definition of the number of possible or concerned persons an incident did or might affect must not exclude products apart from bestselling products. The amount must consider the market conditions and include products from relevant small or medium-sized enterprises (SME) or Start-ups. The requirement of the intensity and quantity should stand-alone. Article 6 par. 2 (d) should require taking into account the intensity *or* the ability to affect a plurality of persons.

(3) Article 6 additional criterion to paragraph 2 CRA: Critical products with digital elements

The approach of a risk assessment in article 6 par. 2 ignores the potential harms an incident can have on an individual. While the approach might consider products particularly risky, which could have a rather small impact on many consumers; it would be ignorant of a potentially great harm to an individual. Targeted attacks such as identity theft are particularly detrimental. Unauthorised persons regularly misuse the identities of consumers in various areas. They use stolen credentials to subscribe to payed services, set up user accounts or order and pay goods.[24] The damages are not limited to high financial losses but rather create a long-term threat to the digital integrity of a person that consumers cannot restore easily. These individual risks must be included in an assessment.

INCLUSION OF POTENTIAL HARM TO INDIVIDUALS

The risk assessment must consider the impact of a possible incident on an individual consumer. The severity is composed of financial damages as well as detriments to the physical and psychological integrity.

3.2 Annex III CRA: Class I

The lack of consumer perspective in the risk assessment generates a list of high-risk products that focuses mainly on industrial uses. However, certain consumer IoT products require stricter certification. Class I must include products that fulfil safety or health functions as well as products collecting sensitive personal data and products designed for children.

Annex III Class I must include security and safety devices, connected toys and other children-accessible devices, smart-home devices as well as health appliances and wearables.

ADDITION OF CONSUMER PRODUCTS IN CLASS I

Class I must include high-risk consumer products. Among them are safety and security devices such as smart locks, alarms and cameras or smoke detectors as well as smart home tools especially if they control essential functions such as heating, venti-

[24] Verbraucherzentrale: Welche Folgen Identitätsdiebstahl im Internet haben kann, 2022, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750, 02/11/2022

lation or electricity. Furthermore, class I must cover wearables such as fitness trackers or smart watches and lastly all devices that are designed for children including for example toys, baby monitors or educational devices.

4. CERTIFICATION AND CONFORMITY ASSESSMENT

Certification and conformity assessments provide orientation and accountability for consumers. They enable consumers to evaluate certain features of a product, compare different producers or versions and indicate that common standards are applied. Oftentimes they are the only available source of information consumers can consult. Without a visible and accessible certificate, the cybersecurity of a product would not be evident to consumers.

vzbv welcomes that particularly risky products are subject to stricter certification and conformity assessment procedures. However, the authenticity of certificates varies depending on the given procedures and involved parties. The awarding certification body must be on the one hand competent and on the other hand impartial and independent from the commissioning company.

A self-declaration however can and must not be put on par with third party certification. Consumers must be able to distinguish a self-declaration easily from an independent certification. It is important not to raise false impressions and provide a comprehensible and transparent information on the parties and tests involved in a certification process. In case that a certificate deviates from the “gold-standard” of independent third-party certification, consumers must be able to understand the restrictive significance in relation to the applied certification.

4.1 Article 8 CRA: Artificial Intelligence Act (AIA)

Art. 8 CRA defines the relation of cybersecurity requirements to the legal obligation concerning the use of artificial intelligence regulated in the Artificial Intelligence Act (AIA).[25] The requirements mainly entail rules for the certification of products with digital elements employing artificial intelligence (AI).

Art. 8 CRA refers to Art. 6 AIA defining the underlying rules for the classification of high-risk AI systems. According to Art. 6 par. 1 (b) AIA high risk AI systems include products that are subject to Union harmonisation legislation and have to pass a conformity assessment procedure by a notified body. This means that regarding the CRA, the AI regulation will only consider products that are subject to third party certification as high risk. An IoT device, employing AI will only be subject to the regulations of high risk products in the AIA if it falls under the critical products with digital elements listed in Annex III CRA. Moreover, critical products from class I do not require external conformity assessment if they apply harmonised standards. That is not comprehensible since the risks regarding connected devices increases when combined with an AI system. A digital product with an AI system considered as high risk according to Art. 6 AIA must require stricter certification rules and should not be assessed by the producer alone.

[25] European Commission: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final) (hereafter ‘AIA’) (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, 02/11/2022

THIRD PARTY CERTIFICATION FOR CONNECTED PRODUCTS USING AI

Connected products and digital services drawing on AI solutions must undergo a mandatory third party certification as defined in Module C and Module H in Annex VI CRA. This mitigates AI-related risks in connected products and protects AI systems from cybersecurity vulnerabilities and potential misuse or manipulation.

4.2 Article 24 paragraph 1 CRA: Conformity assessment procedures

vzbv welcomes that all producers have the possibility to present their product to a third-party certification. The safest way to avoid security risks before a product is placed on the market and used by consumers is in-depth testing by independent third parties. The CRA must provide the provisions to make third party certification feasible for all manufacturers and providers. Third party certification should not be reserved for Big Tech companies that have the financial and human resources to undergo an external assessment. To avoid market distortions, small and medium-sized companies must be supported in an external certification process.

THIRD PARTY CERTIFICATION MUST BE FEASIBLE FOR ALL PRODUCERS

All manufacturers must have the possibility to undergo an external certification process. The CRA must consider obstacles such as limited financial and human resources and support small and medium-sized businesses in certification.

4.3 Article 24 paragraph 2 CRA: Harmonised standards

According to Art. 24 par. 2 a critical product of Class I, Annex III CRA is compliant with the cybersecurity requirements if a producer applies existing harmonised standards. In this case, conformity is presumed, and no external certification is intended. Only if no harmonised standards are available, or if a producer did not apply them, a third-party certification is mandatory.

This is not sufficient for critical products. Class I includes product categories which are high risk such as Virtual Private Network (VPN) clients and password managers, but also products that are essential to the functioning of a device and system such as operating systems or routers. In this case, the CRA must prioritise prevention and make a thorough and independent assessment mandatory.

The process laid down in Art. 24 par. 2 (a) allows a plausibility check by a notified body (Module B and C, Annex VI, CRA). This check of the type of a product certifies that it meets the requirements set out in the CRA and a monitoring of the production process provide a solid and reliable framework to ensure the security of critical devices.

MANDATORY THIRD-PARTY CERTIFICATION FOR ALL CRITICAL PRODUCTS

Critical products must always undergo an external certification. Class I products must undergo an independent plausibility check as provided for in Art. 24 par. 2 (a) (Module B and C).

5. MARKET SURVEILLANCE AND ENFORCEMENT

vzbv welcomes that the proposal of the CRA defines a clear system of national responsibilities under the surveillance of European Union Agency for Cybersecurity ENISA and allows cooperation between member states. It is important to pool resources to be able to oversee the whole market of IoT products. Researchers are essential in coordi-

nated vulnerability discloses since they actively find and report incidences or vulnerabilities.[26] However, the CRA does not draw on all possible resources since it does not embed civil society, science and research as well as consumers and consumer organisations itself. The reporting of security flaws in software or hardware of IoT products is crucial to uphold a high level of cybersecurity. Security researchers, the producer and market surveillance authorities must cooperate to face emerging new threats and detect vulnerabilities.

5.1 Article 11 CRA: Reporting obligations

vzbv welcomes clear and extensive reporting obligations for producers to support an active exchange and profit from learnings. Producers are often reluctant to share vulnerabilities fearing that imitators can exploit the weakness or that they have to share classified information. Ensuring that producers can fix vulnerabilities before unauthorized persons can find and exploit them is important for security. The technical information about a vulnerability must not be abused or fall into the wrong hands. However, if an actor already actively exploited the vulnerability or the producer has detected an incident, they must warn the concerned consumers and the users of a product containing the vulnerability. This notice helps consumers to assess the situation and safeguard their devices but does not have to entail all the technical backgrounds. If no update is available yet, an affected user could for instance still decide to disconnect their device from the network.

While Art. 11 par. 1 clearly defines information obligations of producers towards ENISA, there is no precise provision to inform users about an incident. Art. 11 par. 4 should adopt the 24-hour notification period in order to inform consumers and raise awareness. Producers must not leave users in the dark so that they are able to take actions and restore their safety. Timing is critical in order to prevent possible consequential damage and avert harm from consumers.

> **24-HOUR NOTIFICATION OBLIGATION TO CONSUMERS**
>
> Producers must notify consumers immediately, at the latest within 24 hours if they have knowledge of a vulnerability or an incident.

(1) Annex I Section 1 CRA: Essential cybersecurity requirements

Section 1 point 3 (j), of Annex I obliges producers to provide security related information. This allows for any kind of vulnerability handling such as the required coordinated vulnerability disclosure as regulated by Section 2, point (5), of Annex I. However, the paragraph does not include any specific obligation to share the information with relevant market surveillance authorities or consumers. A general publication is precluded by confidentiality and in order to avoid counterfeiting and a further exploitation of a vulnerability as long as the vulnerability persists. Nevertheless, in case of an incident, it is important that producers eventually provide affected consumers or consumer associations access to relevant information in order to assert liability claims.

> **INFORMATION RIGHTS FOR CONSUMERS**
>
> Producers must provide information about an incident to concerned consumers so that they can assess potential damages and assert liability claims. Article 11 par. 4

[26] ENISA: Coordinated Vulnerability Disclosure Policies in the EU, 2022, https://www.ceps.eu/ceps-publications/coordinated-vulnerability-disclosure-policies-in-the-eu/, 03/11/2022

must be complement by information rights of users including technical information on the vulnerability, concerned data and services as well as potential damages.

(2) Annex I Section 2 CRA: Vulnerability handling requirements

Section 2 of Annex I contains crucial obligations for the conduct in case of an incident or a detected vulnerability. These rules will enable producers to quickly mitigate or remedy risks. vzbv welcomes the cooperative and transparent approach of the requirements. The inclusion of coordinated vulnerability disclosure (CVD) in Section 2 point 5 of Annex I is an essential part of a European cybersecurity structure benefitting from exchange with relevant stakeholders. It is essential that the policy integrates research and civil society. Research contributes to the security by finding vulnerabilities and developing solutions and patches. Producers must be required to process vulnerability reports and cooperate with finders.

The creation of a software bill of materials (SBOM) will facilitate the finding of vulnerabilities. It is a significant prerequisite to break down dependencies and benefit from synergies. It contributes to the security of the software supply chain, which has often suffered from opaque software components such as program libraries or copied code elements in the past as for instance the Log4J incident. The zero day exploit in the Java library resulted in an extremely critical threat situation for nearly a third of all web servers worldwide.[27] The situation was highly uncertain, as most companies had no overview of the open source packages on which their own software was based, making it difficult to understand if they were affected. An SBOM will enable producers and businesses to access information on the software components that they use easily and to accelerate their reaction.

This is decisive to issue security updates quickly and restore security for consumers. Section 2 point 4 of Annex I introduces information obligations for producers. It is important that this information reaches concerned consumers. Hence, a public information cannot substitute a targeted contact to affected users. Producers and providers should notify users by displaying a notice on the affected devices or applications.

TARGETED INFORMATION FOR AFFECTED CONSUMERS

Producers must directly inform users about security updates. Information should be easily accessible and findable.

5.2 Article 43 CRA: National market surveillance

vzbv welcomes the cooperative approach of the CRA allowing for different coordinated actions of national market surveillance authorities. It is important that authorities conduct a review of a product if there is sufficient suspicion of a cybersecurity risk. However, Art. 43 par. 1 requires a market review if there is "sufficient cause" without specifying this further, so that market surveillance authorities are given the discretion to decide on what to check and what not. This can lead to inconsistent procedures within the EU. The CRA must therefore provide control mechanisms to check and support the well-functioning of market surveillance. The human and financial resources of authorities are limited. Without the help of research, civil society and consumer organisations, market surveillance authorities may be blind to incidents and risk developments.

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kritische Schwachstelle in Java-Bibliothek Log4j, 2021, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Schwachstelle-log4Shell-Java-Bibliothek/log4j-schwachstelle/log4j.html, 01/11/2022

Without external reports, market surveillance mainly relies on data from producers and manufacturers themselves. This creates a bottleneck where the producer can potentially conceal non-compliant behaviour or incidents that they do not report.

The CRA must align diverse national authorities. The implementation of coordinated vulnerability disclosure policies in the EU shows substantial differences between the Member States.[28] The regulation must therefore ensure that reporting possibilities are open to all actors and reports are proceeded if the producer does not act. In parallel, for individual consumers the report of an incident is complicated and dissuasive making the cooperation with consumer organisations essential.

CREATE CONTROL MECHANISMS FOR CONSUMERS

Civil society organisations, research and science, as well as consumer organisations must have the power to initiate a review by the responsible national market surveillance authorities.

5.3 Representative Actions Directive

Software and hardware vulnerabilities often affect a large number of consumers, but exceed the competence and resources of an individual user. The CRA must therefore provide consumers with an easy way to claim compensation for damages and allow for redress.

Private enforcement of EU legislation complements the enforcement efforts by official authorities. However, individual consumers are overwhelmed and intimidated by the prospect of long and resource intensive legal proceedings. They greatly benefit when consumer organisations enforce their rights in courts complementary to enforcement by competent authorities.[29]

Consumer organisations such as vzbv are familiar with the detriments consumers are facing in digital markets and can take proactive action. In doing so, they prevent harm from consumers and avoid disputes as far as possible. The European Commission points to the large number of injunction procedures in Germany and Austria “which both traditionally rely on the private enforcement of consumer law initiated by the consumer and business organisations”.[30] The representation by consumer organisations helps to reduce infringements by companies and to diminish adverse effects on consumers.[31]

vzbv successfully settles more than half of its legal actions against companies out of court issuing cease-and-desist declarations.[32] The class-action suit of vzbv against

[28] ENISA: Coordinated Vulnerability Disclosure Policies in the EU, 2022, https://www.ceps.eu/ceps-publications/coordinated-vulnerability-disclosure-policies-in-the-eu/, 03/11/2022

[29] Verbraucherzentrale Bundesverband: Mehr Sammelklage wagen - Kurzpapier des vzbv (2021), https://www.vzbv.de/pressemitteilungen/mehr-sammelklage-wagen, 03/11/2022

[30] European Commission: Report of the Fitness Check SWD(2017)209, https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2017)209&lang=en, 03/11/2022

[31] Ibid. p.103

[32] Verbraucherzentrale Bundesverband: Broschüre: Recht durchsetzen, Verbraucher stärken (2015), https://www.vzbv.de/publikationen/broschuere-recht-durchsetzen-verbraucher-staerken, 03/11/2022

Volkswagen resulted in a €830 million settlement for 200,000 German consumers affected by the emissions scandal.[33] Other proceedings of vzbv against Facebook and Google illustrate the importance of enforcement activities by consumer organisations in the field of data protection.[34] The enforcement of consumer rights by consumer organisations also facilitates and reduces enforcement activities by responsible authorities. It frees up authorities' resources allowing them to focus scarce resources on strategically important cases.

ENSURING PRIVATE ENFORCEMENT

Representative action must be able to enforce cybersecurity requirements. Therefore the CRA must be added to Annex I of the European Directive on representative actions for the protection of the collective interests of consumers ((EU)2020/1828).[35]

6. FINES AND PENALTIES

Today, manufacturers and developers of IoT products and digital services mainly pursue functionality concerns. Security only plays a subordinate role in product development and is considered as a brake in a market dominated by "first-mover" advantage.[36] The CRA is a chance to change this attitude and shift the priority in the direction of security.

This rethinking can only be successful with effective tools for enforcement and implementation. Without adequate fines, the competent authorities will remain a paper tiger and the security of products with digital elements will eventually stagnate.

In order to ensure compliant behaviour, the CRA must define proportionate fines and penalties. Art. 53 par. 3 sets the maximum fines at 15 million Euro respective 2,5 percent of the total worldwide annual turnover. The level is rather low, compared to fines laid down in other regulation. The General Data Protection Regulation (GDPR) allows for maximum fines of four percent (20 million Euro) (Art. 83, par. 5, GDPR).[37] Most recent legislation even increased the threshold. The Artificial Intelligence Act as well as

[33] Volkswagen AG: European Directive on representative actions for the protection of the collective interests of consumers ((EU) 2020/1828) (2020), https://www.volkswagenag.com/en/news/2020/02/vzbv-and-volkswagen-agree-on-a-fair-settlement-solution.html#, 03/11/2022

Verbraucherzentrale Bundesverband: vzbv-Klage gegen VW führt zu Deutschlands größtem Massenvergleich (2020), https://www.vzbv.de/urteile/vzbv-klage-gegen-vw-fuehrt-zu-deutschlands-groesstem-massenvergleich, 03/11/2022

[34] Verbraucherzentrale Bundesverband: Europäische Verbraucherorganisationen gehen gegen Google vor (2022), https://www.vzbv.de/pressemitteilungen/europaeische-verbraucherorganisationen-gehen-gegen-google-vor, 03/11/2022

Verbraucherzentrale Bundesverband: vzbv gegen Facebook: EU-Generalanwalt stärkt Verbandsklagen (2021), https://www.vzbv.de/meldungen/vzbv-gegen-facebook-eu-generalanwalt-staerkt-verbandsklagen, 03/11/2022

[35] 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, 03/11/2022

[36] European Commission: Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715 (2021), https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products, 03/11/2022

[37] European Parliament: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1667483054631, 03/11/2022

the Digital Services Act (DSA) set fines up to six percent of the total worldwide annual turnover. [38]

The maximum fines can be charged for violations of the basic cybersecurity requirements. When it comes to misinformation, the penalties are even lower with a maximum penalty of one percent or five million Euro. Since the fines define maximum penalties, actual fines will be in most cases much lower. The maximum sentence must therefore leave more room in order to act as an effective deterrent.

SET HEAVY PENALTIES TO DETER NON-COMPLIANCE

The CRA should align with the AIA and DSA and set maximum fines at six percent of the total worldwide annual turnover.

[38] European Commission: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final) (hereafter 'AIA') (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, 02/11/2022

European Parliament: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1667483451431, 02/11/2022