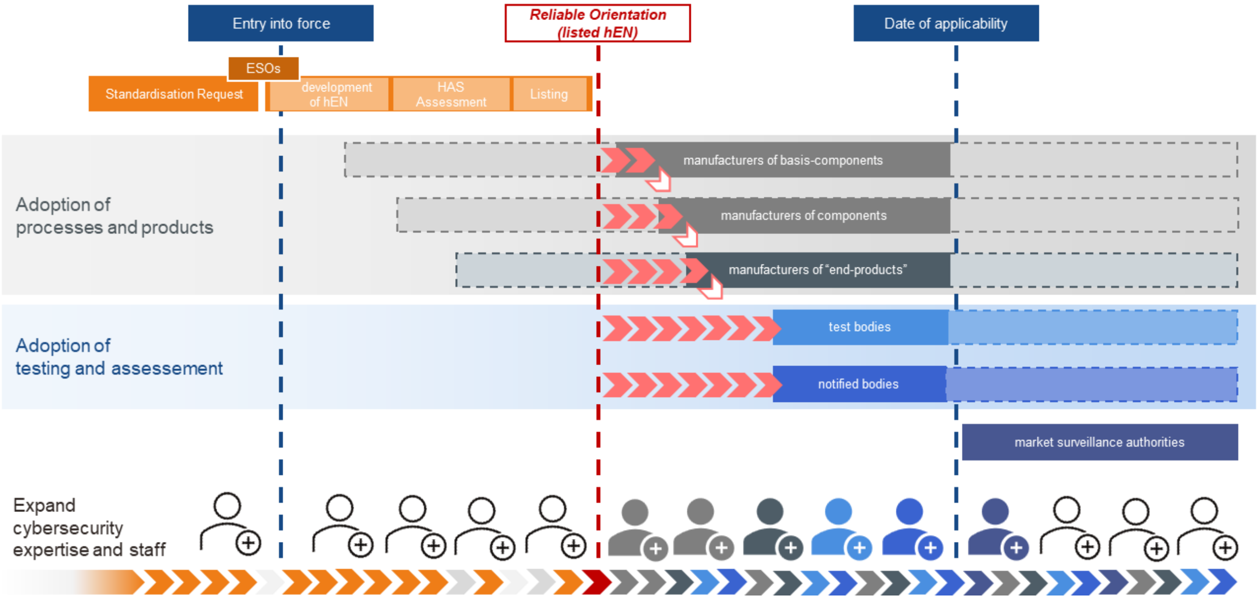
ZVEI-Pager

Cyber Resilience Act (CRA)

In the light of the proliferation of a fragmented regulatory landscape regarding cybersecurity, the ZVEI is a strong long-time proponent for a horizontal cybersecurity regulation for products within the proven new legislative framework (NLF).[1] Therefore, we welcome in principle the coherent proposal of the CRA, as it follows the logic of the NLF and only adds some needed limited requirements in the life cycle, especially the establishment of a vulnerability management process, in a considerate manner.

Our positions

- **Make the CRA the central reference point for** product **cybersecurity requirements and align the interplay with other regulations**, including those of the new machinery regulation (esp. reg. Annex III, section 1.1.9), the GPSR and the AI-Act. Also include the repeal of the delegated act under article 3 (3) d,e,f of the radio equipment directive (RED) in the text of the CRA to avoid double regulation.
- **Ensure a realistic transitional period and transition strategy**, potentially through a staggered approach, for a successful implementation through the cascade (comp. fig), including the development of hEN, their fast assessment and listing.


Entry into force
Reliable Orientation (listed hEN)
Date of applicability
ESOs
Standardisation Request
development of hEN
HAS Assessment
Listing
Adoption of processes and products
manufacturers of basis-components
manufacturers of components
manufacturers of "end-products"
Adoption of testing and assessment
test bodies
notified bodies
market surveillance authorities
Expand cybersecurity expertise and staff

- **Clarify the definitions & scope of the regulation**: Focus on products, which are really able to exchange data (bidirectionally); Add an **exemption regarding spare parts** to allow for the continuous use of long living goods. Add missing definitions and streamline and clarify the content of the regulation to **ensure unambiguity** for the development of the harmonized standards (hEN) as well as for the economic actors concerned.
- **Choose a more differentiated approach to critical products with digital elements by amending the too broad classification in annex III** and differentiate between components and systems. Delete art. 6 (5) and encompass "highly critical products" in the third-party conformity assessment procedures acc. to art. 24 (3).
- **Optimize the connection of the obligations to the manufacturer and essential requirements for an effective and efficient implementation.** Especially amend essential cybersecurity requirement 1 (2) in annex I to reference the vulnerability handling requirements and not to address hypothetical vulnerabilities of products during transit, which will be fixed by the process requirements, e.g. through initial security updates
- **Conformity assessment – strengthen the consistent NLF-Approach of the CRA**; other means of showing conformity, like common specifications and CSA-Schemes, should undergo similar obligations and quality safeguards as hEN. Allow for the prudent (re)-use of established international standards like IEC 62443 in the development of the hEN.

[1] Comp. first whitepaper from 2018 on this topic Horizontal Product Regulation for Cybersecurity (Whitepaper) - zvei.org, which in essential parts became the German industry position on the topic: EU-wide Cybersecurity Requirements (bdi.eu)

- Mitigate possible additional challenges through the CRA in already strained supply chains, by taking into account the **incomplete character of most components**, especially in regard to their conformity assessment and testing and through the introduction of a lower limit for components, which pose only minimal risk.
- **Align the reporting obligations for incidents and vulnerabilities with the NIS-2-directive** and limit those requirements to significant incidents having a significant impact and actively exploited vulnerabilities. Refer to already established international reference points and scoring systems like the MITRE reference-method for "common vulnerabilities and exposures" (CVE) and the CISA "known exploited vulnerabilities catalog" (KEV).

Current state

- **Complex regulatory landscape regarding cybersecurity,** which can be divided in regulations, which address operations and in those, which address products. Concerning the cybersecurity of operations, the current Network and Information Security directive (NIS) will be superseded by the overhauled NIS-2-directive with effect from 18 October 2024. The cybersecurity of products is partly addressed in different, mostly newly (re-)worked, sectoral regulations in context of other protection goals (new machinery regulation; general product safety regulation; AI Act; proposal of the new product liability directive and the radio equipment directive (RED)). The product regulations as well as the regulation for the operation side have connections to the voluntary certification framework of the 2019 cybersecurity act.
- The **delegated act under Art. 3(3) d,e,f of the RED plays a special role** as its date of application, 1st of august 2024; will precede the CRA and through this regulatory effort the first cybersecurity requirements for products falling under the RED will be established.
- To simplify the complex regulatory landscape and to counter the further proliferation of piecemeal cybersecurity requirements, the European Commission has proposed the Cyber Resilience Act on the 15th of September 2022, which is currently under discussion by the European co-legislators and is planned to enter into force under the current commission.

Background: Numbers & Facts

- **Critical personnel gap**: Currently are already more than **100,000 cybersecurity professionals missing** for Germany alone. Other European member states have similar numbers, e.g. France and Spain with about 60,000 missing experts in relation to a **worldwide gap of 3,4 million cybersecurity workers**[2]. And the raised demand through NIS-2, the delegated act under the RED and the CRA isn't fully considered yet.
- **Continuous proliferation of connected devices:** The number of IoT-devices will increase even more in the upcoming years, reaching a range of over 30 billion predicted IoT connections in 2028 from currently over 13 billion connections.[3]
- **Uninterrupted high threat landscape:** Cybercrime is still a profitable field of activity for malicious actors**,** and the threat level rises in spite of efforts of national authorities and industry and some increases in overall cybersecurity awareness. E. g. the number of new malware variants registered by the German BSI has increased about 116,6 million to over 1 billion.[4] Also the last year saw the largest Denial of Service (DDoS) attack ever, launching in Europe.[5] For those attacks the trend is recognized, that they were often launched from compromised servers or consumer devices, such as Internet-of-Thing (IoT) products and broadband routers. Often caused by delays in updating and patching the compromised devices.[6] This ambivalence regarding updates is underscored by a ZVEI poll with over 1500 participants, which shows that under two-thirds of respondents said they regularly install updates on IT and communications devices. In relation to the owners of networkable consumer electronics, their share is only 43%, and 32% for networkable household appliances.

Contact

Marcel Hug • Manager Cyber Security & Strategy • Digital and Innovation Policy •
Tel.: +49 69 6302 432 • Mobil: +49 162 2664 941 • E-Mail: Marcel.Hug@zvei.org

ZVEI e. V. • Electro and Digital Industry Association • Lyoner Straße 9 • 60528 Frankfurt am Main • Germany
Lobbying Register ID.: R002101 • EU Transparency Register ID: 94770746469-09 • www.zvei.org 02/2023

[2] (ISC)2 Cybersecurity Workforce Study, 2022; p. 3 & 8. The staff shortage does not seem to have fully reached the wages for this group in Europe, as the corresponding U.S. wage level is significantly higher (about 40%) than the European one. (ebd. p. 65).

[3] 13,2 billion total connections in 2022 to a forecast of 34,7 billion IoT connections in 2028 (combined number of wide, area, cellular and short range IoT connections); Ericsson Mobility Report, November 2022, p. 11.

[4] BSI-Lagebericht: Die Lage der IT-Sicherheit in Deutschland 2022; p. 13, 52.

[5] Threat Landscape — ENISA (europa.eu)

[6] [6] ENISA TREAT LANDSCAPE 2022, November 2022, p. 71.