At a glance

Cyber Resilience Act (CRA)

Initial situation

The CRA, as a supplement to the Cybersecurity Act (CSA), aims to meet market needs and make digital products more secure. This is to be achieved by introducing horizontal cybersecurity rules for industry stakeholders, in particular producers of tangible and intangible digital products and ancillary services. In this context, a groundbreaking regulation at EU level is imminent, which directly affects us as a digital economy.

Bitkom’s view

Taking steps into the right direction: We welcome the creation of a more efficient regulatory framework to improve cybersecurity. The CRA offers the opportunity to take a coherent approach at European level to close regulatory gaps that lead to security gaps in the digital value chain and to eliminate conflicting or overlapping regulations.

Core points

Therefore, Bitkom is of the opinion that the CRA should primarily pursue the following goals:

- **Extending the scope of the security obligations to the life cycle of digital products**

  Digital products - hardware, software and the combination thereof - are partly integrated in highly complex systems. Consequently, regulation must take interactions into account in order to ensure a high level of security for digital infrastructures throughout the entire product life cycle. Regulatory obligations must be placed where control measures are most effective - in the interaction between manufacturers and users. In this context, it is important to offer both market players and supervisory authorities the necessary legal security.

- **Improve the consistency of the legal framework for cybersecurity according to the principles of the NLF**

  A reduction of complexity between different, often sectoral regulatory approaches through the policy option of horizontal regulation according to the principles of the NLF is supported. The use of harmonised standards has a long and successful history in EU product legislation under the NLF.

- **Consistency of requirements with existing legal acts**

  The CRA offers the possibility of reducing complexity between different, often sectoral, regulatory approaches to cyber security of products and harmonising the regulatory landscape under a single, horizontal, consistent and coherent reference point.

- **Alignment with international requirements**

  If national standards exist, they should be aligned with international standards, as these have been extensively validated and are based on consensus-based information and guidance for defining and implementing effective security methods. As ICT standardisation is already global in nature, an existing, already effective standardisation infrastructure can be used for this purpose.

Bitkom's Position

The expansion of services in the digital sphere and the increasing dependence on digital products have significantly increased cyber threats. Even though security measures are constantly being adapted to these new challenges, criminal efforts are becoming more sophisticated and increasingly digital. Cyber security is therefore a key prerequisite for a successful digital economy and society. As a result, cybersecurity requirements have been progressively introduced through a growing number of existing or proposed legislative acts regulating products or organisations (e.g. Cyber Security Act, Radio Equipment Directive RED 2014/53/EU, Network and Information Systems Security Directive (NIS Directive) Directive (EU) 2016/1148, European Medical Devices Regulation MDR Regulation (EU) 2017/745). Despite these efforts, we see that the regulatory framework for the European digital market remains fragmented. Different economic actors also face different levels of regulation. Addressing cybersecurity under different conditions across multiple legal instruments inevitably leads to legal uncertainties and a heavy, unnecessary burden on businesses. Consequently, this will continue to create significant security gaps in the digital business value chain.

Bitkom therefore welcomes the EU Commission's initiative to create a more efficient legal framework for cyber security by introducing legislation on horizontal requirements. From our point of view, the upcoming Cyber Resilience Act (CRA) offers the European Union the great opportunity to take a coherent approach. This involves defining clear, harmonised rules that follow a risk-based approach. The CRA legislative process offers the opportunity to both streamline the legal rules and make their implementation more efficient. Therefore, the aim should not only be to adopt an additional layer of regulation, but also to merge contradictory or overlapping regulations into a single piece of legislation. This should be done in line with internationally recognised standards and avoid overly prescriptive requirements and inconsistencies with other EU legislation. For the EU Digital Single Market, its businesses and consumers, the current legislative process offers the opportunity to achieve a higher level of security by closing the regulatory gaps in the value chain and making regulation more efficient and easier to apply. The establishment of a single horizontal CRA also offers the possibility of clear and effective market surveillance, which is essential for enforcing cybersecurity requirements.

The regulation must be drafted with great care, as it will have a massive impact on the European Single Market and its competitiveness.

Angelina Marko
Fachreferentin
Industrie4.0 &
Technische Regulierung

T +49 30 27576-133
a.marko@bitkom.org

Bitkom e.V.
Albrechtstraße 10
10117 Berlin

In Bitkom's view, the CRA should therefore primarily focus on the following issues:

Extending the scope of the security obligations to the life cycle of digital products

The basic prerequisite for the trouble-free functioning of highly digitalised processes, networked products and services is a high degree of cyber resilience. In particular, it is important to note that products - hardware, software as well as combinations thereof - are partly integrated into highly complex systems. This poses a legal challenge, as all these elements will be very difficult to cover in a one-fits-all approach. Consequently, attention must also be paid to interactions in regulation. The goal must be to ensure a high level of security for digital infrastructures for consumers and businesses. In doing so, it is important to offer both market players and supervisory authorities the necessary legal certainty in equal measures. Thus, in Bitkom's view, a uniform set of cybersecurity regulations should be provided for all products that are currently subject to EU product regulation, without unduly restricting the scope for efficient and economically viable implementation. This approach should encompass all IoT devices relevant to a cybersecure society. In particular, the CRA should therefore focus exclusively on networked digital products in its scope.

Bitkom is of the opinion that manufacturers of hardware and software are already implementing "security-by-design" responsibly. However, in a dynamic security environment, fixed-point-in-time test conditions on the product can only guarantee security to a limited extent. In order to future-proof the CRA, the CRA must define fundamental security objectives that also extend beyond the product itself. During the expected life cycle of a product, it must therefore be ensured that security updates are regularly made available and installed by the user. However, it is essential that the duration of the life cycle is defined by the manufacturer and communicated transparently to the users.

Increasing awareness and best practices around product development, vulnerability management and transparency around security software updates can reduce major security risks, in our view.

Improve the consistency of the legal framework for cybersecurity according to the principles of the NLF

Bitkom supports the option of horizontal regulation according to the principles of the New Legislative Framework (NLF) as an important step towards a harmonised and higher level of security, more legal certainty and consistency across the digital market. Here, it is necessary to assess the centrality of a component, a digital product as well as its scope of application and the degree to which it is brought to market. Based on the intended use of the product and a risk assessment, more specific requirements or more demanding conformity assessment procedures can be used.

The selection or assignment of conformity evaluation procedures for products covered by such a regulation must therefore be carefully considered. Decision 768/2008/EC offers a variety of different procedures for this purpose, from which the legislator is to select the appropriate ones. Bitkom prefers self-assessment by the manufacturer as long as there is no good reason for the mandatory involvement of a third party (high risk). Safety regulations in the form of harmonised standards for products have been shown to be an efficient and risk-based approach to ensure safety for consumers and other end-users. The use of harmonised standards has a long and successful history in EU product legislation under the NLF. The main advantage is that general legal requirements can be described in detail at the technical level, allowing effective incorporation of sector-specific needs, in addition to the horizontal requirements set by the CRA. Based on the broad scope of the CRA, Bitkom recommends using this approach. In doing so, the self-assessment underlines the principle that manufacturers must confirm and be responsible for the security - in this case cyber security - of their products. Companies that choose to involve third parties for conformity assessment should also be able to do so. In this regard, it is important to note in the CRA that a flexible mechanism must be provided to avoid duplication of effort and to ensure a modular approach to the use of conformity assessment procedures. This applies equally to products and application environments where complementary or higher requirements are required.

In our view, it is thus also important that the CRA, in addition to the basic requirements for products, can also set obligations for manufacturers that go beyond mere product manufacturing. This approach is in line with product regulation under the New Legislative Framework (NLF) and takes into account the need for compliance before and after products are placed on the market or entered into service.

However, in our view, conformity assessment - both self-determined and by third parties - can only bring about an increase in cybersecurity if it is supported by effective market surveillance. Reducing the number of unlawful market participants who create competitive advantages for themselves through insufficient compliance efforts is crucial to achieve the goals. Sanctions against non-compliant market participants must be severe and thus have a deterrent effect. This also applies to the independent conformity assessment bodies involved.

Consistency of requirements with existing legal acts

It will be essential for the EU to ensure coherence with existing, forthcoming and revised sectoral legislation. Currently, the legislative landscape is characterised by fragmentation and the parallel coexistence of national and European cybersecurity laws. The complexity of the regulatory environment is further increased by the fact that there is no clear distinction between the roles and obligations of manufacturers, sellers and operators, the definition of products and services and their respective responsibilities in the value chain.

Bitkom identifies the target as reducing complexity between different, often sectoral, regulatory approaches to cybersecurity of products and harmonising the regulatory landscape under a central, consistent and coherent reference point. Cybersecurity requirements in other EU product regulations must be avoided and already adopted legislation or relevant provisions should be replaced or repealed, as an example the delegated act activating Articles 3.3 d, e and f (Cybersecurity) of the RED.

Alignment with international requirements

We see an appropriate policy option in future regulations that include harmonised European standards. In this context, it is important to establish self-assessment as the standard conformity assessment procedure. This should be complemented by the possibility to require third party assessments for a certain category of high-risk products. Should national standards exist, they should be aligned with international standards, as these have been extensively validated and are based on consensus-based information and guidance for the definition and implementation of effective safety methods. This can ensure that a collaborative approach to common challenges is used, enabling global cooperation and interoperability.

As ICT standardization is already global in nature and the involvement of all stakeholders is enormously important, an existing, already effective standardization infrastructure with ISO/IEC JTC1, CEN/CLC/JTC 13, ETSI TC CYBER and other bodies can be used here.

Bitkom represents more than 2,700 companies in the digital economy, including more than 2,000 direct members. These companies generate annual sales of 190 billion euros with IT and telecommunications services - including exports of 50 billion euros. Bitkom members employ more than 2 million people in Germany. Members include more than 1,000 SMEs, over 500 startups and almost all global players. They offer software, IT services, telecommunications or Internet services, manufacture devices and components, are active in the field of digital media or are otherwise part of the digital economy. 80 percent of the companies are headquartered in Germany, 8 percent each come from Europe and the USA, and 4 percent from other regions. Bitkom promotes and drives the digital transformation of the German economy and advocates broad social participation in digital developments. The aim is to make Germany a leading global digital location.

Bitkom e. V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org