Cyber Resilience Act

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Such products suffer from two major problems adding costs for users and the society:

1. a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
2. an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs.

Two main objectives were identified aiming to ensure the proper functioning of the internal market:

1. create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product’s life cycle; and

2. create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Four specific objectives were set out:

1. ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;
2. ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
3. enhance the transparency of security properties of products with digital elements, and
4. enable businesses and consumers to use products with digital elements securely.

Downloads

1. Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber

resilience Act (.pdf)
Download

2. Annexes Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act (.pdf)
Download

Related topics

Cybersecurity European Cybersecurity Competence Centre

Related content

New EU cybersecurity rules ensure more secure hardware and software products

Press release | 15 September 2022

The Commission presented yesterday a proposal for a new Cyber Resilience Act to protect consumers and businesses from products with inadequate security features.

Cyber Resilience Act - Impact assessment

Report / Study | 15 September 2022

This Impact Assessment accompanies the proposal for a Regulation on cybersecurity requirements for products with digital elements, the Cyber Resilience Act.
