CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity

#SOTEU

2022

SEPTEMBER 2022

A first ever EU wide legislation of its kind: the **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle.

The Act will

- Ensure that **products with digital elements** placed on the EU market have **fewer vulnerabilities** and that manufacturers remain **responsible for cybersecurity** throughout a product's life cycle;
- **Improve transparency** on security of hardware and software products;
- Business users and consumers benefit from **better protection.**

Every 11 seconds there is a
ransomware attack

Ransomware attacks alone are estimated to have cost the world roughly **€20 billion** in 2021

The **global annual cost** of cybercrime was estimated to be **€5.5 trillion** in 2021

Manufacturer's obligations

Cybersecurity is taken into account in **planning, design, development, production, delivery** and **maintenance** phase;

All **cybersecurity risks** are documented;

Manufacturers will have to **report actively exploited vulnerabilities and incidents**;

Once sold, manufacturers must ensure that for the **expected product lifetime** or for a period of five years (whichever is the shorter), **vulnerabilities are handled effectively**;

Clear and understandable instructions for the use of products with digital elements;

Security updates to be made **available for at least five years**.

EU standards based on the Cyber Resilience Act will facilitate its implementation and will be an asset for the EU cybersecurity industry in global markets.

The Cyber Resilience Act complements European cybersecurity rules and strengthens the security of the whole supply chain.

Harmonised rules for the placing on the market of connected hardware and software products;

Essential cybersecurity requirements for the design and development of products with digital elements as well as obligations for all economic operators in the value chain;

Harmonised rules for the duty of care for the whole life cycle of products with digital elements.

Timeline

The European Parliament and the Council will examine the proposed Cyber Resilience Act.

Once adopted, **economic operators and Member States will have two years to adapt to the new requirements**. The obligation to report actively exploited vulnerabilities and incidents will apply after one year.

The Commission will **periodically review the Cyber Resilience Act and report** on its functioning.

How the Cyber Resilience Act will work in practice

#SOTEU

2022

90% of products	10% of products	
Default category	**Critical "Class I"**	**Critical "Class II"**
Self-assessment	Application of a standard or third-party assessment	Third-party assessment
Criteria: n/a	**Criteria:** • **Functionality** (e.g. critical software) • **Intended use** (e.g. industrial control/NIS2) • **Other criteria** (e.g. extent of impact) **Critical products**	

Examples

- Photo editing
- Word processing
- Smart speakers
- Hard drives
- Games
- ... etc.

Examples (Annex III)

- Password managers
- Network interfaces
- Firewalls
- Microcontrollers
- ... etc.

Examples (Annex III)

- Operating systems
- Industrial firewalls
- CPUs
- Secure elements
- ... etc.