Cyber Resilience Act: MEPs adopt plans to boost security of digital products

- More robust cybersecurity for all products with digital elements
- Covers everyday products like connected doorbells, baby monitors and Wi-Fi routers
- Security updates to be applied automatically when technically feasible

On Tuesday, Parliament approved new cyber resilience standards to protect all digital products in the EU from cyber threats.

The regulation, already agreed with Council in December 2023, aims to ensure that products with digital features are secure to use, resilient against cyber threats and provide enough information about their security properties.

Important and critical products will be put into different lists based on their criticality and the level of cybersecurity risk they pose. The two lists will be proposed and updated by the European Commission. Products deemed to pose a higher cybersecurity risk will be examined more stringently by a notified body, while others may go through a lighter conformity assessment process, often managed internally by the manufacturers.

During the negotiations, MEPs made sure that products such as identity management systems software, password managers, biometric readers, smart home assistants and private security cameras are covered by the new rules. Products should also have security updates installed automatically and separately from functionality updates.

MEPs also pushed for the European Union Agency for Cybersecurity (ENISA) to be more closely involved when vulnerabilities are found and incidents occur. The agency will be notified by the member state concerned and receive information so it can assess the situation and, if it
identifies a systemic risk, will inform other member states so they are able to take the necessary steps.

To emphasise the importance of professional skills in the cybersecurity field, MEPs also introduced education and training programmes, collaborative initiatives, and strategies to enhance workforce mobility in the regulation.

**Quote**

Lead MEP Nicola Danti (Renew, IT) said: “The Cyber Resilience Act will strengthen the cybersecurity of connected products, tackling vulnerabilities in hardware and software alike, making the EU a safer and more resilient continent. Parliament has protected supply chains ensuring that key products such as routers and antiviruses are a priority for cybersecurity. We have ensured support for micro and small enterprises, better involvement of stakeholders, and addressed the concerns of the open-source community, while staying ambitious. Only together will we be able to tackle successfully the cybersecurity emergency that awaits us in the coming years.”

**Next steps**

The legislation was approved with 517 votes in favour, 12 against and 78 abstentions. It will now have to be formally adopted by Council, too, in order to come into law.

**Background**

New technologies come with new risks, and the impact of cyber-attacks through digital products has increased dramatically in recent years. Consumers have fallen victim to security flaws linked to digital products such as baby monitors, robot-vacuum cleaners, Wi-Fi routers and alarm systems. For businesses, the importance of ensuring that digital products in the supply chain are secure has become pivotal, considering three in five vendors have already lost money due to product security gaps.

**Further information**

Adopted text (12.03.2024)
Video recording of the debate (11.03.2024)
Committee on Industry, Research and Energy
Procedure file
EP research briefing
Legislative train
Contacts

Baptiste CHATAIN
Press Officer
📞 (+32) 498 98 13 37
✉️ baptiste.chatain@europarl.europa.eu
✉️ indu-press@europarl.europa.eu
🐦 @EP_Industry