State of the Union: New EU cybersecurity rules ensure more secure hardware and software products

Brussels, 15 September 2022

Today, the Commission has presented a proposal for a new Cyber Resilience Act to protect consumers and businesses from products with inadequate security features. A first ever EU-wide legislation of its kind, it introduces mandatory cybersecurity requirements for products with digital elements, throughout their whole lifecycle.

The Act, announced by President Ursula von der Leyen in September 2021 during her State of the European Union address, and building on the 2020 EU Cybersecurity Strategy and the 2020 EU Security Union Strategy, will ensure that digital products, such as wireless and wired products and software, are more secure for consumers across the EU: in addition to increasing the responsibility of manufacturers by obliging them to provide security support and software updates to address identified vulnerabilities, it will enable consumers to have sufficient information about the cybersecurity of the products they buy and use.

Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age, said: "We deserve to feel safe with the products we buy in the single market. Just as we can trust a toy or a fridge with a CE marking, the Cyber Resilience Act will ensure the connected objects and software we buy comply with strong cybersecurity safeguards. It will put the responsibility where it belongs, with those that place the products on the market."

Margaritis Schinas, Vice-President for Promoting our European Way of Life, said: "The Cyber Resilience Act is our answer to modern security threats that are now omnipresent through our digital society. The EU has pioneered in creating a cybersecurity ecosystem through rules on critical infrastructure, cybersecurity preparedness and response, and the certification of cybersecurity products. Today, we are completing this ecosystem through an Act that brings security in everyone's home, in all our businesses and in every product that is interconnected. Cybersecurity is a matter for society, no longer an industry affair."

Thierry Breton, Commissioner for the Internal Market, said: "When it comes to cybersecurity, Europe is only as strong as its weakest link: be it a vulnerable Member State, or an unsafe product along the supply chain. Computers, phones, household appliances, virtual assistance devices, cars, toys... each and every one of these hundreds of million connected products is a potential entry point for a cyberattack. And yet, today most of the hardware and software products are not subject to any cybersecurity obligations. By introducing cybersecurity by design, the Cyber Resilience Act will help protect Europe's economy and our collective security."

With ransomware attacks hitting an organisation every 11 seconds around the globe and the estimated global annual cost of cybercrime reaching €5.5 trillion in 2021 (Cybersecurity Ventures as quoted in Joint Research Centre report (2020): "Cybersecurity – Our Digital Anchor, a European perspective"), ensuring a high level of cybersecurity and reducing vulnerabilities in digital products – one of the main avenues for successful attacks – is more important than ever. With the growth in smart and connected products, a cybersecurity incident in one product can have an impact on the entire supply chain, possibly leading to severe disruption of economic and social activities across the internal market, undermining security or even becoming life-threatening.

The measures proposed today are based on the New Legislative Framework for EU product legislation and will lay down:
(a) rules for the placing on the market of products with digital elements to ensure their cybersecurity;

(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products;

(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes. Manufacturers will also have to report actively exploited vulnerabilities and incidents;

(d) rules on market surveillance and enforcement.

The new rules will rebalance responsibility towards manufacturers, who must ensure conformity with security requirements of products with digital elements that are made available on the EU market. As a result, they will benefit consumers and citizens, as well as businesses using digital products, by enhancing the transparency of the security properties and promoting trust in products with digital elements, as well as by ensuring better protection of their fundamental rights, such as privacy and data protection.

While other jurisdictions around the world look into addressing these issues, the Cyber Resilience Act is likely to become an international point of reference, beyond the EU's internal market. 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 proposed regulation will apply to all products that are connected either directly or indirectly to another device or network. There are some exceptions for products, for which cybersecurity requirements are already set out in existing EU rules, for example on medical devices, aviation or cars.

**Next Steps**

It is now for the European Parliament and the Council to examine the draft Cyber Resilience Act. Once adopted, economic operators and Member States will have two years to adapt to the new requirements. An exception to this rule is the reporting obligation on manufacturers for actively exploited vulnerabilities and incidents, which would apply already one year from the date of entry into force, since they require fewer organisational adjustments than the other new obligations. The Commission will regularly review the Cyber Resilience Act and report on its functioning.

**Background**

Cybersecurity is one of the Commission’s top priorities and a cornerstone of the digital and connected Europe. An increase of cyber-attacks during the coronavirus crisis has shown how important it is to protect hospitals, research centres and other infrastructure. Strong action in the area is needed to future-proof the EU's economy and society. It is estimated that the annual costs of data breaches are at least €10 billion and the annual costs of malicious attempts to disrupt traffic on the internet are estimated to be at least €65 billion (impact assessment report accompanying the Commission Delegated Regulation supplementing Radio Equipment Directive Delegated Regulation).

The Cybersecurity Strategy, presented in December 2020, has proposed to integrate cybersecurity into every element of the supply chain and bring further together EU's activities and resources across the four communities of cybersecurity – internal market, law enforcement, diplomacy and defence. It builds on the EU' Shaping Europe's Digital Future and the EU Security Union Strategy, and leans on a number of legislative acts, actions and initiatives the EU has implemented to strengthen cybersecurity capacities and ensure a more cyber-resilient Europe.

The new Cyber Resilience Act will complement the EU cybersecurity framework: the Directive on the security of Network and Information Systems (NIS Directive), the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), which was recently agreed by the European Parliament and the Council, and the EU Cybersecurity Act.

**For More Information**

Questions and Answers: EU Cyber Resilience Act
Factsheet on the EU Cyber Resilience Act
Proposal for a Cyber Resilience Act
Factsheet on the new EU Cybersecurity Strategy
Factsheet on the Proposal for a Directive on measures for high common level of cybersecurity across the Union (NIS2 Directive)

Factsheet on Cybersecurity: EU External Action

Questions and Answers: New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient

Proposal for a Directive on measures for high common level of cybersecurity across the Union (NIS2 Directive)

Proposal for a Directive on the resilience of critical entities

IP/22/5374

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

Related media

Cybersecurity