Proposal for directive on measures for high common level of cybersecurity across the Union

The Commission has adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive).

In spite of its notable achievements, the Directive on the security of network and information systems (NIS Directive), which paved the way for a significant change in mind-set, institutional and regulatory approach to cybersecurity in many Member States, has by now also proven its limitations. The digital transformation of society (intensified by the COVID-19 crisis) has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses.
Now any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market.

To address these challenges, as announced in the Communication on Shaping Europe's Digital Future, the Commission accelerated the Directive's review to the end of 2020, carried out an impact assessment and presented a new legislative proposal.

Key elements of the Commission proposal

The new Commission proposal aims to address the deficiencies of the previous NIS Directive, to adapt it to the current needs and make it future-proof.

To this end, the Commission proposal expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope. At the same time, it leaves some flexibility for Member States to identify smaller entities with a high security risk profile.

The proposal also eliminates the distinction between operators of essential services and digital service providers. Entities would be classified based on their importance, and divided respectively in essential and important categories with the consequence of being subjected to different supervisory regimes.

The proposal strengthens security requirements for the companies, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied. The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

Furthermore, the Commission proposes to address security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships. At the European level, the proposal strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA, will carry out coordinated risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks.

The proposal introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

The proposal also enhances the role of the Cooperation Group in shaping strategic policy decisions on emerging technologies and new trends, and increases information sharing and cooperation between Member State authorities. It also enhances operational cooperation including on cyber crisis management.

The Commission proposal establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creating an EU registry on that operated by the European Union Agency for Cybersecurity (ENISA).

Next Steps

Relevant next steps actions are:

- The Proposal will be subject to negotiations between the co-legislators, notably the Council of the EU and the European Parliament
- Once the proposal is agreed and consequently adopted, Member States will have to transpose the NIS2 Directive within 18 months.
- The Commission has to periodically review the NIS2 Directive and report for the first time on the review 54 months after the entry into force.
- The European Commission looks forward to implementing the new Cyber strategy in the coming months.

Downloads

1- Proposed directive on measures for a high common level of cybersecurity across the Union (.pdf)
Download

2- Annex to the Proposed directive on measures for a high common level of cybersecurity across the Union (.pdf)
Download

Related topics

Cybersecurity
Strengthening trust and security

Related content

Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union

Policy and legislation | 16 December 2020

-