NIS2 Directive: securing network and information systems

Cybersecurity involves protecting **network and information systems** (NIS), their users, and other affected individuals from cyber incidents and threats. To respond to the increased exposure of Europe to cyber threats, Directive 2022/2555, also known as NIS2 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555), replaced its predecessor, Directive 2016/1148 or NIS1. NIS2 raises the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools. It requires Member States to **enhance their cybersecurity capabilities**, while introducing risk management measures and reporting requirements to entities from more sectors and setting up rules for cooperation, information sharing, supervision, and enforcement of cybersecurity measures.

The directive mandates that each Member State adopt a national cybersecurity strategy, which includes policies for supply chain security, vulnerability management, and cybersecurity education and awareness. Member States must also establish and regularly update a list of operators of essential services, ensuring these entities comply with the directive's requirements.

In addition to the sectors already covered by NIS 1 - energy, transport, healthcare, finance, water management, and digital infrastructure - the new rules also apply to providers of public electronic communications, more digital services (such as social platforms), waste and wastewater management, critical product manufacturing, postal and courier services, and public administration at both central and regional levels, as well as the space sector. As a rule, medium-sized and large entities in these critical sectors, will have to take appropriate cybersecurity risk-management measures and notify relevant national authorities of significant incidents. These are incidents that could cause significant disruption or damage.

The directive also includes provisions for supervision, enforcement, and voluntary peer reviews to enhance mutual trust and cybersecurity capabilities across the EU. It also introduces accountability of the top management for non-compliance with cybersecurity risk management measures thus bringing cybersecurity to the attention of the boardroom.

The directive sets up a network of Computer Security Incident Response Teams (CSIRTs) (https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/csirts-network) to exchange information on cyber threats, and respond to incidents. These teams are crucial for maintaining situational awareness and offering assistance. To manage large-scale cybersecurity incidents or crises, the directive creates the European cyber crisis liaison organisation network (EU-CyCLONe) (https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone). This network supports coordinated management and ensures regular information exchange among Member States and EU institutions in case of large-scale incidents and crises.

In parallel, the NIS Cooperation Group (https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group) is a platform established by the NIS Directive to facilitate strategic cooperation and information exchange among EU Member States, the European Commission, and the EU Agency for Cybersecurity (ENISA). The group publishes non-binding guidelines and recommendations to support the implementation of the NIS Directive.

Background

The NIS 1 (Directive 2016/1148) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148) was the first comprehensive EU legislation aimed at boosting cybersecurity of network and information systems to safeguard vital services for the EU's economy and society. In December 2020, the Commission proposed revising NIS 1, resulting in the adoption of NIS 2, which came into force in January 2023. Member States had until 17 October 2024 to transpose the NIS2 Directive into national law. NIS 2 repealed NIS1 as from 18 October 2024.