Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

The NIS2 directive

A new avatar on EU-wide cybersecurity

Introduction

The first EU-wide law on cybersecurity, the NIS Directive, came into force in 2016 and helped achieve a higher and more even level of security of network and information systems across the EU. In view of the unprecedented digitalisation, new rules have been introduced to ensure stronger cybersecurity. This is termed as the 'NIS 2 directive' on measures for a high common level of cybersecurity across the Union. The NIS 2 Directive is introduced to ensure a safer and stronger Europe by significantly expanding the sectors and type of critical entities falling under its scope. These include providers of public electronic communications networks and services, data centre services, wastewater and waste management, manufacturing of critical products, postal and courier services and public administration entities, as well as the healthcare sector more broadly. Furthermore, the NIS 2 is looked-upon to strengthen the cybersecurity risk management requirements that companies are obliged to comply with, as well as streamline incident reporting obligations with more precise provisions on reporting, content, and timeline. The NIS 2 Directive replaces the rules on the security of network and information systems, the first EU-wide legislation on cybersecurity.

What does NIS 2 mean for companies

In September 2022, the Commission adopted the proposal for Cyber Resilience Act, which lays down cybersecurity requirements for products with a digital element, covering both hardware and software. Under the NIS 2 Directive, companies will have to take appropriate and proportionate technical, operational, and organisational measures to manage the cybersecurity risks, prevent and minimise the impact of potential incidents. This requirement becomes much more concrete under NIS 2 with a list of focused measures including among others:

- incident response and crisis management,
- vulnerability handling and disclosure,
- policies and procedures to assess the effectiveness of cybersecurity risk management measures, and
- cybersecurity hygiene and training

The NIS 2 directive emphasises increased information-sharing and cooperation on cyber crisis management at both national and EU levels, the Directive streamlines incident reporting obligations with more precise provisions on reporting, content, and timeline. Furthermore, there are more stringent supervisory measures for national authorities, as well as stricter enforcement requirements, along with the list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations.

NIS 2 Directive: Things to know

The NIS2 Directive aims to address the deficiencies of the previous rules, to adapt it to the current needs and make it future-proof. The Directive expands the scope of the previous rules by adding new sectors based on their degree of digitalisation and interconnectedness and how crucial they are for the economy and society, by introducing a clear size threshold rule— meaning that all medium and large-sized companies in selected sectors will be included in the scope. At the same time, it leaves certain discretion to Member States to identify smaller entities with a high security risk profile that should also be covered by the obligations of the new Directive.

The new Directive eliminates the distinction between operators of essential services and digital service providers. Entities would be classified based on their importance, and divided into two categories: essential and important entities, which will be subjected to different supervisory regime. It strengthens and streamlines security and reporting requirements for companies by

imposing a risk management approach, which provides a minimum list of basic security elements that have to be applied. The new Directive introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

NIS2 addresses security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in the supply chains and supplier relationships. At European level, the Directive strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA, may carry out Union level coordinated security 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 Directive introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States. It also enhances the role of the Cooperation Group in shaping strategic policy decisions and increases information sharing and cooperation between Member State authorities. It also enhances operational cooperation within the CSIRT network and establishes the European cyber crisis liaison organisation network (EU-CyCLONe) to support the coordinated management of large-scale cybersecurity incidents and crises. NIS 2 also establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creates an EU vulnerability database for publicly known vulnerabilities in ICT products and ICT services, to be operated and maintained by the EU agency for cybersecurity (ENISA).

Increased EU-wide Cyber Cooperation

The NIS 2 directive is advocating increased cooperation among the EU member states and suggested for an establishment of a European Cyber crisis liaison organisation network (EU-CyCLONe) supporting coordinated management of large scale cybersecurity incidents and crisis at EU-level. This organisation network shall assist in coordinated vulnerability disclosure as well. In addition, streamlined incident reporting obligations, with more precise provisions on the reporting process, content, and timeline, especially for operators of essential services (OES) and Digital Service providers (DSP), as these are critical for citizens. In short, NIS 2 directive is providing measures for a high common level of cybersecurity across the European Union. NIS2 Directive is closely linked with two other initiatives, the Critical entities Resilience (CER) Directive and the Regulation for the Digital Operational resilience for the financial sector (Digital Operational Resilience Act, DORA).

More specifically, Member States will be able to jointly supervise the implementation of EU rules and mutually assist each other in the case of cross-border malpractices, have a more structured dialogue with the private sector and coordinate the disclosure of vulnerabilities found in software and hardware sold across the internal market. They will also be able to work in a coordinated manner to assess the security risks and threats related to new technologies, as done for the first time with 5G. The EU wide cooperation to improve national capabilities through staff exchanges between authorities and peer reviews shall be advanced. The existing groups, notably the Cooperation Group gathering national cybersecurity authorities and the Network of Computer Security Incident Response Teams (CSIRTs) will contribute to advance cooperation respectively at both strategic and technical levels. The DORA competent authorities would be able to consult and share relevant information with the Single Point of Contacts (SPOCs) and CSIRTs established under NIS2. The competent authorities, SPOCs or the CSIRTs established under NIS2 would also receive details of major ICT-related incidents from the competent authorities under DORA.

NIS 2 expanding the cyber sectoral landscape

1. Expanding scope of new sectors as critical sectors: The NIS 2 Directive replaces the NIS Directive and thus expands the scope to so-called essential and important entities in sectors of high criticality listed in Annex I and other critical sectors listed in Annex II introducing a size-cap rule as a general rule.

Annex 1

Energy	
Transport	
Financial market infrastructure, banking	
Drinking water, wastewater	
Digital Infrastructure	• Internet Exchange Point providers • DNS Service providers • TLD name registers • Cloud computing service providers • Content delivery network providers • Trust service providers • Providers of public electronic communications networks
ICT service management (B2B)	• Managed service providers • Managed security service providers
Public administration	
Space	

Annex 2

Postal and courier services	
Waste Management	
Manufacture, production and distribution of chemicals	
Production, processing and distribution of food	
Manufacture of medical devices, certain electronic products as well as machinery and transport	
Digital Providers	• Providers of online marketplaces • Providers of online search engines • Providers of social networking service platforms
Research	

2. New Requirements: The NIS 2 introduces new requirements such as

a. Registration requirements for all entities falling within the scope of NIS 2 directive

b. Requirement of certain measures such as:

- i. measures regarding incident handling,
- ii. business continuity,
- iii. supply chain security,
- iv. human resources security,
- v. access control policies and
- vi. asset management

c. Greater reporting requirements: The new directive follows a graduated approach with respect to notification of significant incidents to the CSIRT or, where applicable, the competent authority

d. Risk Management Governance: The management bodies of essential and important entities will be required to approve and oversee the implementation of the cybersecurity risk-management measures.

e. Accountability of Top Management: The NIS 2 introduces accountability and liability of top management for the non-compliance with cybersecurity obligations, more stringent supervisory measures for national authorities as well as stricter enforcement requirements. In addition, administrative fines have been introduced.

Recommendations for companies

The NIS 2 directive shall make more work for the companies in terms of checks and balances and also for their suppliers and the following list shall help companies to understand what actions are required at their end.

Look for new requirements to be implemented by the organisation

Whether the organisation deals with suppliers or customers subject to the new rules;

Obligations required to be attributed to suppliers, to facilitate cybersecurity compliance and other applicable legislative act;

Prepare/update processes for incident and threat reporting;

Insight into the regulatory obligations of Member states

Assess the Commission's implementing acts for harmonisation of additional cybersecurity requirements across the EU;

Look for any related or additional local IT security requirements, and steer for a coordinated implementation approach