kaspersky bring on the future

The EU NIS 2 Directive: New obligations and what you can do to prepare for them

What is the NIS 2 Directive about?

The NIS 2 Directive[1] went into force on January 16th, 2023, and Member States will have to transpose the Directive by October 17, 2024. In addition to other goals, the NIS 2 Directive requires the main operators in key industries to take security measures and report incidents.

Who does NIS 2 apply to?

An entity is covered by the scope of the directive if it operates in one of the sectors and types of services listed in the annexes of the Directive and if it is of a certain size. For all the details, exceptions and nuances, see the Articles 2 & 3 and Annexes I & II of the Directive[2]. NIS 2 Directive establishes two categories for entities within its scope: essential entities and important entities. Both categories must adhere to the same requirements. The differentiation lies in the supervisory measures and penalties.

What are the NIS 2 cybersecurity requirements?

According to Article 21 (1) of the Directive Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services.

These measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- Policies on risk analysis and information system security;
- Incident handling;
- Business continuity, such as backup management and disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- Basic cyber hygiene practices and cybersecurity training;
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- Human resources security, access control policies and asset management; the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive); https://eur-lex.europa.eu/eli/dir/2022/2555

[2] https://eur-lex.europa.eu/eli/dir/2022/2555

What are the penalties for non-compliance?

The competent authorities may impose significant administrative fines for violations of the obligations under the national legislation transposing the NIS 2 Directive. These fines may amount to a maximum of up to €10 million or 2% of the worldwide annual turnover of the group of companies in the case of essential companies or entities, or up to €7 million or 1.4% of the worldwide annual turnover of the group in the case of important companies or other entities.

How should companies start preparing? Recommendations

Companies and other entities should start preparing now by:

- Assessing whether and to what extent you will be subject to the cybersecurity obligations under the NIS 2 Directive
- Check the transposition of the NIS Directive into national law in your member state
- Follow the information and recommendations of your national cybersecurity authorities[3]
- Assess and further develop the technical, operational and organizational measures to manage the risks posed to the security of network and information systems

How Kaspersky's solutions and services can help your business?

As a cybersecurity vendor, Kaspersky leverages all of its expertise to help organizations build robust cyber defenses. We can support you with the following solutions and services:

Endpoint Detection and Response (EDR) is a technical solution that provides deep insights into what is happening on your endpoints. With Kaspersky Endpoint Detection & Response (EDR) Optimum you can proactively scan your server and client network for specific Indicators of Compromise (IoC). Your IT or an external service provider gains insightful knowledge about impending cyberattacks and can take immediate action if required. In the event of an incident, you will receive important data for root cause analysis.

Managed Detection and Response (MDR) allows you to outsource your cyber protection to our experienced experts. Kaspersky's threat hunters monitor telemetry data from your IT systems and immediately detect suspicious activity. This 24/7 service is provided by specialists located in various Security Operations Centers (SOC) around the world.

Awareness training: Kaspersky has developed an effective overall concept for building up cyber security expertise within the company. The spectrum ranges from general training to sensitize and motivate your team, to specialist training for help desk staff and online training for managers. Our interactive online training platform, KASAP, offers practical security awareness training for your team that can be easily integrated into the daily work routine. Participants can flexibly work through the learning modules online and repeat them at any time.

Threat Intelligence (TI): Industry-leading (TI) provides organizations with a 360-degree view of the threat landscape. It gives them access to Kaspersky's comprehensive threat database and expert knowledge of the IT and OT environment. This enables them to detect imminent attacks early, strengthen security measures and harden their systems.

Incident Response (IR): In the event of a security incident, well-prepared organizations have the advantage of being able to respond more quickly and efficiently. Kaspersky offers a range of incident response services to help organizations prepare for an emergency. For example, Kaspersky Tabletop Exercise (TTX) is a guided exercise that allows you to review your incident response processes and plans. You will identify gaps in your emergency plan, clarify team roles and responsibilities, and improve coordination between departments.

Industrial Cybersecurity: Kaspersky Industrial Cybersecurity (KICS) is a proven and certified industrial solution that addresses the specific cybersecurity needs of industrial enterprises and critical infrastructure operators. KICS already protects more than 1,000 high-end industrial customers worldwide.

Kaspersky understands the needs of different industries and company sizes and **protects over 220,000 companies worldwide** against cyber threats. Kaspersky's reliable all-in-one cyber protection covers multiple protection dimensions.

Protect now!

[3] See for example the recommendations by NCSC Ireland: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf ; French ANSSI: https://www.ssi.gouv.fr/directive-nis-2/ ; or CCB Belgium: https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization#_Toc128118851

Cyberthreat News: securelist.com/
Kaspersky Blog: kaspersky.co.uk/blog/
Cybersecurity for large enterprises: kaspersky.com/small-to-medium-business-security
Cybersecurity for mid-size companies: kaspersky.com/enterprise-security

kaspersky.com