Kaspersky Security Awareness

Ensuring Compliance with the European NIS 2 Directive with Kaspersky Security Awareness

The European NIS 2 Directive ((Directive (EU) 2022/2555), also known as the Network and Information Systems Security Directive, aims to enhance cybersecurity across Europe by ensuring that organizations take appropriate measures to protect their networks and information systems.

In-scope essential and important organizations include those in the following sectors:

Essential

- Energy
- Transportation
- Banking and financial infrastructures
- Healthcare
- Drinking water and wastewater
- Digital infrastructure
- Public administration
- Space

Important

- Postal and courier services
- Waste management
- Chemical manufacturing, production, and distribution
- Food production, processing, and distribution
- Manufacturing of medical, electronic, transportation, or related equipment
- Digital providers
- Research

* Member states may extend NIS2 requirements to organisations that do not meet these personnel or revenue criteria but that do play a key role in supporting the health, safety, and/or stability of the EU.

NIS 2 Basics

By 17 October 2024, Member States must adopt and publish the measures necessary to comply with the NIS 2 Directive.

Who must comply with the Directive

The Directive imposes specific obligations on certain companies, including operators of essential services (OES) and digital service providers (DSPs), to implement robust cybersecurity measures and report incidents to national authorities. It clearly lists all the sectors and subsectors (industries) that need to comply with this European cybersecurity directive.

Member states must identify and impose NIS2 requirements on all organizations in their jurisdiction that:

1. Employ at least 50 people or generate at least €10,000,000 in revenue*
2. Provide services deemed “essential” or “important” to the health, safety, and/or stability of the EU

Why is NIS 2 important?

NIS 2 is important because it sets very strict cybersecurity requirements for a large number of companies in the European Union – by some estimates, more than 100,000 companies in the European Union will have to become NIS 2 compliant.

Even though NIS 2 does not apply to as many companies as, e.g. the EU GDPR, it will certainly become a de facto standard for critical infrastructure that other (non-EU) countries will emulate – a very similar scenario has happened already in non-EU countries with privacy regulations that are very similar to the EU GDPR.

NIS 2 fines and liabilities

For companies that are not NIS 2 compliant, the fines are as follows:

> For essential entities – up to **10 million** euros or **2%** of the total annual turnover.
> For important entities – up to **7 million** euros or **1.4%** of the total annual turnover.

It is important to note that Article 20 requires the top management of essential and important entities to approve the cybersecurity risk management measures and oversee their implementation, and it specifies that top management can be held liable if cybersecurity is not compliant with Article 21.

Key points of the Directive:

1. Implementing appropriate technical and organizational measures to ensure network and information system security
2. Reporting significant cyber incidents to national authorities
3. Providing appropriate training to staff on cybersecurity awareness
4. Conducting regular risk assessments and implementing incident response plans
5. Collaborating with other organizations and sharing threat intelligence to enhance cybersecurity resilience

What the Directive says about training:

One of the key requirements of the NIS 2 Directive is to provide appropriate training to their staff on cybersecurity awareness. This training should cover topics such as identifying and responding to cybersecurity threats, protecting sensitive data, and adhering to cybersecurity policies and procedures. By ensuring that employees are well-informed about cybersecurity best practices, organizations can reduce the risk of cyber incidents and enhance their overall security posture.

How Kaspersky Security Awareness helps:

Kaspersky Security Awareness is a comprehensive solution that empowers employees with essential cybersafety skills to help organizations to protect themselves from human-related incidents, and to create a cybersafety culture inside organization, thereby complying with the requirements of the NIS 2 Directive. With a range of interactive modules, quizzes, and simulations, Kaspersky Security Awareness enables organizations to instill cybersecurity best practices in their employees, in an engaging and effective manner.

Benefits of using Kaspersky Security Awareness:

Upskill employees

Training raises awareness about cybersecurity threats and the importance of following security protocols.

Reduce human error

A significant number of security breaches are due to human error. Effective training can reduce these incidents.

Foster a culture of security

Regular training sessions help to establish a culture of security within the organization.

To learn more about Kaspersky Security Awareness, please visit our website or contact our team for a personalized consultation. Together, we can work towards enhancing cybersecurity across Europe and ensuring the security of critical networks and information systems.

Stay ahead of cyberthreats with Kaspersky Security Awareness.

Conclusion:

Compliance with the European NIS 2 Directive is crucial for organizations in critical sectors to protect their networks and information systems from cyberthreats. By implementing robust cybersecurity measures and providing comprehensive staff training, organizations can enhance their cybersecurity resilience and reduce the risk of cyber incidents. Kaspersky Security Awareness is a proven solution for organizations looking to meet the requirements of the Directive and improve their overall security posture.

kaspersky bring on the future

www.kaspersky.com