ELEARNINGNEWS ARTICLE

Year 8 - number 298 Wednesday 17 July 2024

NIS2 regulation: how to comply by October 2024

The NIS2 is the updated European cybersecurity regulation that came into force in January 2023, replacing the previous NIS1.

In today's digital landscape, **cybersecurity** is no longer an option but an essential necessity. With increasingly sophisticated cyber threats, the protection of data and infrastructures has become a priority for companies and organizations across all sectors. For this reason, the European Union introduced the **NIS2 Directive**, a significant evolution of the previous NIS1, aimed at strengthening Europe's resilience against cyber threats.

NIS1: a solid starting point

The NIS1 Directive, which came into effect in 2016, represented a significant step forward in the European cybersecurity landscape. It introduced security measures for critical sectors such as **energy**, **transport**, and **financial infrastructures**. However, with the advancement of digitalization and the increase in cyber threats, there emerged the need to establish a more robust and comprehensive regulatory framework.

NIS2: new security measures for the digital era

NIS2, which came into force on **January 17 2023**, responds to this need decisively and concretely. It introduces new and stricter security measures for a wide range of sectors, including **healthcare**, **postal services**, and **wastewater**.

What does NIS2 introduce?

Here are some key points of NIS2:

- **A wider scope**. The new regulation applies to a larger number of sectors and activities, ensuring more comprehensive and uniform protection.
- **New categories of operators**. Two new categories are introduced: Essential Service Operators (ESOs) and Digital Service Providers (DSPs). The former are public or private entities providing critical services for society such as energy, transport, healthcare, and water. The latter are entities providing digital services to a significant number of users in the EU, such as online platforms, cloud services, and electronic communications.
- **Stricter risk management obligations**. NIS2 requires organizations to implement more rigorous and structured risk management measures, such as cybersecurity planning, incident management, and notification.
- **Increased reporting obligations**. The regulation imposes even more imperative requirements for organizations to promptly report serious cybersecurity incidents to the competent authorities.
- **Stronger penalties**. NIS2 introduces stricter penalties for organizations that fail to comply with its obligations, encouraging adherence to the regulation and protection of cybersecurity.

NIS2: which companies are affected?

NIS2 applies to a wide range of companies and organizations, including:

- **Operators in critical sectors**: energy, transport, healthcare, finance, wastewater, public sector.
- **Digital service providers**: email, search engines, cloud computing.
- **Online platforms**: marketplaces, social media.

NIS2: by when do you need to comply?

The deadline to comply with NIS2 is October 18, 2024. Affected companies must therefore act promptly to implement the necessary security measures and comply with the new regulation.

How to prepare for NIS2

To prepare for NIS2, companies should follow some fundamental steps:

1. **Assess your situation**. It is necessary to identify the sectors in which the company operates, the sensitive data it handles, and the potential risks it faces.
2. **Conduct a risk assessment**. An in-depth analysis of the threats and vulnerabilities to which the company is exposed is essential to define adequate security measures.
3. **Implement security measures**. It is important to adopt the necessary technical and organizational measures to mitigate the identified risks, based on industry standards and best practices.
4. **Test and monitor**. The implemented security measures must be regularly tested to verify their effectiveness and constantly monitored to adapt to evolving threats.

Besides these fundamental steps, here are some additional suggestions for companies:

- **Appoint a cybersecurity officer**. This figure will be responsible for overseeing the implementation and maintenance of security measures.
- **Train staff on cybersecurity.** All employees should be aware of cyber threats and know how to protect company data and infrastructures.
- **Use reliable security solutions**. Invest in state-of-the-art cybersecurity solutions to effectively protect company infrastructures and data from constantly evolving cyber threats.

Advanced cybersecurity solutions

Here are some practical examples of how **cutting-edge cybersecurity technologies** can help companies comply with NIS2:

- **Intrusion detection and prevention systems (IDS/IPS)**. These systems monitor network traffic and identify suspicious activities that may indicate an ongoing attack.
- **Next-generation firewalls (NGFW)**. They offer more advanced protection than traditional firewalls by filtering traffic based on more granular criteria and protecting against the latest threats.
- **Encryption solutions.** These protect sensitive data both during storage and transmission, making it inaccessible to hackers.
- **Identity and access management (IAM) solutions.** These solutions control who can access company resources and what they can do, ensuring that only authorized users have access to data and systems.
- **Backup and recovery solutions.** In the event of a cyber attack, it is crucial to have complete and up-to-date backups of company data to quickly restore them.

NIS2: an opportunity for companies

Beyond investing in technological solutions, it is also important to invest in **staff training on cybersecurity**. Employees are often the weakest link in cybersecurity, so it is essential to make them aware of cyber threats and how to protect themselves.

In conclusion, compliance with NIS2 is not just a regulatory obligation but also a significant investment for companies: it can be an **opportunity to improve their cybersecurity, increase customer trust, and strengthen their competitiveness.**