LOGPOINT

Getting started with NIS2

www.logpoint.com

INTRO

NIS2 is an EU directive adopted by the EU parliament in November 2022. It aims to protect critical infrastructure within the EU from cyber threats and to achieve a high level of security across the EU. Building upon the 2016 NIS directive, NIS2 includes stricter security requirements, reporting obligations, and enforcement requirements for a broader scope of organizations.

The EU Network and Information Security (NIS) 2 directive aims to strengthen organizations' security posture to address emerging cyber threats.
Logpoint can help your business increase cybersecurity and comply with the regulation

NIS2 has strengthened security requirements, including:

- Incident response and crisis management
- Vulnerability handling and disclosure
- Supply chain security
- Policies and procedures to assess the effectiveness of cybersecurity risk management
- Basic computer hygiene practices and cybersecurity training
- The effective use of cryptography
- HR security, access control policies, and asset management

What if I don't comply with NIS2?

Much like the GDPR directive that came into effect in 2018 to safeguard personally identifiable information, NIS2 introduces reporting obligations and administrative sanctions for noncompliance and failure to report incidents. Sanctions under NIS2 include orders to implement the recommendations of a security audit, orders to bring security into line with NIS requirements, and administrative fines of up to €10m or 2% of the worldwide turnover of an organization.

When will NIS2 be in effect?

The EU parliament adopted NIS2 on November 10, 2022. It is an EU directive that governments will be required to implement into national law within 21 months, which means organizations that operate in the EU must comply with the requirements by mid-2024.

Is NIS2 applicable to your organization?

NIS2 will apply to many organizations operating critical infrastructure, including public authorities and private companies:

- Energy (electricity, oil, gas, district heating, and hydrogen)
- Transport (air, rail, water, and road)
- Banking, Financial market infrastructure)
- Healthcare (including labs and research on pharmaceuticals and medical devices)
- Drinking water and wastewater processing
- Digital Infrastructures (Telecom, DNS, TLD, datacentres, trust services, cloud services)
- Digital services (search engines, online markets, social networks)
- Public administration
- Space industry
- Postal and courier service
- Waste management
- Chemicals (production and distribution)
- Food (production, processing, and distribution)
- Science and education

HOW LOGPOINT CAN HELP WITH NIS2 COMPLIANCE

The Logpoint Converged SIEM solution is an end-to-end security operations platform that combines SIEM, SOAR, UEBA, endpoint agent monitoring and response, and the ability to detect and respond to threats in business-critical systems. Logpoint reduces the time to detect and respond across the entire threat landscape all from one unified interface.

Logpoint provides the three key components to NIS2 compliance:

1. Supply chain security

NIS2 requires that companies consider cybersecurity risks in the supply chain of their information and communication technology. Logpoint takes cybersecurity and security of our software and development processes very seriously which is reflected in our Common Criteria EAL3+ certification. EAL3+ is the highest security standard achieved by any SIEM vendor, which means our products are secure by design, including how we build, evaluate and protect our software. Logpoint also adheres to ISO 15408, and we perform frequent third-party penetration tests and industry security audits, such as SOC 2 Type II. Logpoint is compliant with the strictest data privacy regulations, including GDPR, CCPA and Schrems II, which guarantees data residency in the EU.

2. Reporting

NIS2 requires that businesses submit a report within 24 hours about significant incidents. Logpoint centrally collects logs across your network and infrastructure. With out-of-box reports and an audit record of all changes to the system, it's easy to create and share full incident reports.

3. Detection, response, and Incident handling

After the initial report in 24 hours, NIS2 requires a final report of a major incident within one month. Logpoint has built-in case management that automatically combines related incidents into a single case, helping speed up investigation and response. Logpoint adds relevant information from threat intelligence, enrichment, and other investigations to give a complete picture of what's going on. You can easily create reports directly from each case.

PRACTICAL STEPS YOU SHOULD TAKE

To effectively manage evolving cyber risks and adhere to NIS2, your board and senior management should define or enhance your cybersecurity strategy using the following guide to improve cyber resiliency. Management support is key because NIS2 holds the management level directly responsible for ensuring that NIS2 requirements are met.

Below there are six things you should do to prepare your organization for NIS2:

Perform a maturity assessment

Assess whether NIS2 applies to your organization and what it will take for your organization to comply, either in-house or through an external consultant. The maturity assessment shows what your organization needs to implement or where to improve to meet the requirements. The assessment also evaluates any investments or competencies your company needs to succeed with compliance.

Identify critical assets

NIS2 seeks to protect critical infrastructure, critical infrastructure supply chains, and other societally important functions. NIS2 covers the critical assets in two categories of organizations:

- **Essential entities:** energy, transport, health, water, space, public administration, digital infrastructure, and banking and financial market
- **Important entities:** postal services, manufacturing, and food production, among others.

It's important to identify the operationally critical assets in your organization's processes, people, technologies and suppliers, such as suppliers subject to interference by a non-EU country or state- backed players.

Implement a SIEM or cyber management framework

NIS2 requires that organizations implement an information security management system (ISMS) for cyber and information security. In addition to an ISMS, a SIEM, like Logpoint, provides centralized log management and the ability to detect and respond to incidents, ensuring you meet the requirement Logpoint adheres to information security standards, including ISO27001 to ensure information assets are secure.

Assess risks and implement mitigations

NIS2 requires a risk-based approach to cyber and information security, which means your organization must describe a risk process, comply with it and identify preventative measures to reduce risks. With the help of an information management framework like ISO27001, you should risk assess all critical assets, including your supply chain and suppliers.

Report to CSIRT

NIS2 requires organizations to report incidents to the National Centre for Cyber Security (CSIRT) within 24 hours. Organizations must continuously give status updates and report any compromises. The purpose of the reporting requirement is to increase cyber capabilities across Europe.

Repeat again and again

One of the main points of NIS2 is that organizations must implement a risk process and continuously work on it, similar to information management standards like ISO27001. The cyber landscape is constantly changing, which means the risks are too. Organizations need to assess their cybersecurity policies and procedures regularly to keep their security posture current.

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**