NETWORK INFORMATION SYSTEMS DIRECTIVE (NIS2)

EU Cyber Compliance Advisory

Overview

The Network Information Systems Directive (NIS2) enhances and broadens the scope of the original NIS Directive, increasing sector coverage and strengthening requirements for cybersecurity across various industries. Effective from January 2023, member states have until October 2024 for full implementation.

NIS2 introduces stricter oversight, higher penalties for essential entities, and mandatory incident reporting.

Targeted Bussines Sectors

Essential Entities:

- Energy (electricity, oil, gas)
- Transport (air, rail, water, road)
- Banking
- Financial Market Infrastructures
- Health
- Drinking Water / Waste Water
- Digital Infrastructure
- ICT-Service Management (B2B)
- Public Administration

Important Entities:

- Postal and Courier Services
- Waste Management
- Chemicals (manufacture, production, and distribution)
- Food (production, processing, and distribution)
- Manufacturing (including of computers, electronic and optical products, electrical equipment, machinery, motor vehicles, and transport equipment)
- Digital Providers (including online marketplaces, online search engines, and cloud computing services)
- Research

Challenges & Financial Impact

- Fines of **€10,000,000 or 2% of global annual turnover** for ”essential" entities, and **€7,000,000 or 1.4% of global turnover** for "important" entities.
- Penalties include warnings, binding instructions, and administrative fines.
- Top management can face personal liability for breaches.
- Stricter reporting requirements within 24 hours for significant incidents.
- Increased supervisory measures for essential entities, including on-site inspections.

How Can Stefanini Help

Security Monitoring (NSOC)

Essential for continuous monitoring required by NIS2, which demands entities to have capabilities to detect security incidents on their networks.

Vulnerability Scanning (VMS)

Directly supports NIS2's mandate for regular vulnerability assessments to identify and mitigate risks.

Detection & Response (MDR/MPDR)

Aligns with NIS2's incident response and management provisions.

Proactive Services (Ethical Hacking)

These services help in fulfilling NIS2's requirements for testing and evaluating the effectiveness of cybersecurity risk management measures.

CSIRT

As NIS2 emphasizes incident reporting, having a dedicated CSIRT aligns with the directive's requirements.

Technology Implementation Services

Can be used to implement technical solutions that comply with NIS2's security requirements.

HEADQUARTERS

EMEA - Brussels, Belgium
North America - Southfield, MI, USA
Global - Sao Paulo, Brazil
www.stefanini.com
info@stefanini.com