SOPHOS

Scope, definitions, and context of NIS2 terminology

Scope – Essential Services

"Essential Services" is a defined term of art in the NIS 1 Directive. (Critical to the economy.) The phrase should be used specifically here and capitalized because it refers to specific industry sectors. These were: Energy, Transport, Banking, Financial Market Infrastructure, Health, Drinking Water Supply, and Digital Infrastructure. (7 industry sectors, total, in NIS 1)

NIS 2 changed the phrase to "Essential Entities," kept all of the listed industry sectors, and added Public Administration. Further, NIS 2 added a new category, "Important Entities," also a defined term of art. (Important to the economy but not Critical.) Important Entities are Postal and Courier Services, Waste Management, Manufacture Production and Distribution Channels, Food Product Processing and Distribution, Pharmaceutical Manufacturing Production and Distribution, Medical Device Manufacture Production and Distribution, and Digital Providers. (19 industry sectors, total, in NIS 2)

List of NIS 2 cybersecurity requirements

- **Risk Management**: Organizations are required to implement a comprehensive cybersecurity risk management framework tailored to their operations, including
- **Risk assessment**: Periodic assessments of potential risks to network and information systems
- **Supply Chain Security**: Assessing and managing the security of supply chains
- **Technical and Organizational Management**:
- **Access Control**: Ensuring only authorized individuals can access critical systems.
- **Incident Response**: Establishing a process for detecting, responding, and recovering
- **Security Monitoring**: Continuous monitoring and logging of network and information systems
- **Vulnerability Management**: Proactively identifying vulnerabilities
- **Cryptography**: Using encryption and other cryptographic measures to protect sensitive data
- **Incident Reporting and Response**:
  - Organizations are required to report significant incidents to the relevant national authorities within 24 hours of becoming aware of the incident
  - Detailed incident notifications, including a post-incident report, must be submitted within 72 hours
  - The NIS 2 Directive thresholds determine what comprises a "significant incident"
- **Supply Chain Security**: Entities must address cybersecurity risks in their supply chains and services. This includes assessing suppliers' security practices and incorporating security requirements in contracts.
- **Governance and Accountability**:
  - **Management Oversight**: Senior management is accountable for cybersecurity risk
  - **Cybersecurity Policies**: Organizations must establish internal policies
  - **Training and Awareness**: Regular cybersecurity awareness and training programs
  - **Audits**: Regular audits and security reviews to ensure compliance with NIS 2

Management

- NIS 2 specifically assigns **legal and supervisory responsibilities** to **management bodies**, particularly the **board of directors**, holding **senior management** directly accountable for ensuring compliance with the Directive.
- **Management bodies** are required to **approve cybersecurity risk management measures**, which may include threat protection, software products, and other relevant actions.
- **Incident reporting** is mandated under NIS 2, meaning that the details of any incident must be **captured, understood, and remediated** in accordance with the Directive.

2024-11-08 (PC)

SOPHOS