CyberScope® Addresses Multiple NIS2 Directive Measures

Application Note

CyberScope® Addresses Multiple NIS2 Directive Measures

CyberScope Edge Network Vulnerability Scanner

INTRODUCTION

Organizations across the European Union (EU) face escalating IT threats, from physical disruptions to cyberattacks. Though all aspects of IT are at heightened exposure, one area of significant challenges is the network perimeter. Why? The network edge is frequently ground-zero for many hackers because it offers so many attack vectors:

- **Proliferation of endpoints**
- **Increased attack surfaces**
- **Ubiquitous connectivity**
- **Undetected vulnerabilities**
- **Unsecured connections**
- **Misconfigured networks**

As will be discussed below, the edge network is where NetAlly's CyberScope and Link-Live™ cloud-based collaboration, sharing, and analysis platform can aid EU entities in strengthening their cybersecurity posture and addressing NIS2 Directive measures.

WHAT IS THE NIS2 DIRECTIVE?

NIS2 stands for "Network and Information Security Directive". Here is the official definition*:

> *The NIS2 Directive (Directive (EU) 2022/2555) is a legislative framework designed to enhance cybersecurity across the European Union by establishing a high common level of security for network and information systems. It builds upon the original NIS Directive, expanding its scope and strengthening requirements to better address evolving cyber threats.*
>
> *Under NIS2, essential and important entities must adopt appropriate, proportionate technical, operational, and organizational measures to manage cybersecurity risks. These measures aim to protect network and information systems, as well as to prevent or minimize the impact of incidents on service recipients and interconnected services.*
>
> *The directive mandates an "all-hazards" approach, meaning that entities must be prepared to address a wide range of threats, from cyberattacks to physical disruptions, ensuring comprehensive protection and resilience in their operations.*

Summarizing, the objective of NIS2 is to manage risk and strengthen the security of network and information systems for organizations within the EU by bolstering the cybersecurity resiliency of their critical infrastructure and essential services. The directive includes minimal obligations of entities that must be carried out to protect against cyber threats, and should a breach occur, incident reporting guidelines to relevant authorities.

The NIS2 Directive (Directive (EU) 2022/2555) is a legislative framework designed to enhance cybersecurity across the European Union by establishing a high common level of security for network and information systems.

*NIS2 Directive Training, Updates, Compliance (nis-2-directive.com)

THE NIS2 DIRECTIVE IS NOW LAW

New rules to boost cybersecurity of EU's critical entities and networks[**] are now in effect.

> "…Today's adoption of the implementing regulation coincides with the deadline for Member States to transpose the NIS2 Directive into national law. As of tomorrow, 18 October 2024, all Member States must apply the measures necessary to comply with the NIS2 cybersecurity rules, including supervisory and enforcement measures."
>
> "The implementing regulation will be published in the Official Journal in due course and enter into force 20 days thereafter."

Once enforcement begins, EU entities within the member states required to comply must demonstrate compliance with the NIS2 directive measures. Therefore, it is incumbent these entities begin implementation efforts quickly.

These entities fall into two broad categories, those that provide "essential" or "important" services to the European economy or society. Essential organizations include Transport, Energy, Banking, Health, and Water, while important entities span: Postal and courier services, Waste management, Chemical production and processing, Food, and Digital providers

"…Today's adoption of the implementing regulation coincides with the deadline for Member States to transpose the NIS2 Directive into national law. As of tomorrow, 18 October 2024, all Member States must apply the measures necessary to comply with the NIS2 cybersecurity rules, including supervisory and enforcement measures."

NIS2 CYBERSECURITY MEASURES MINIMAL OBLIGATIONS

The NIS2 Directive Article 21[***], Cybersecurity risk-management measures shall include at least the following (see the appendix for more details):

(a) policies on risk analysis and information system security

(b) incident handling

(c) business continuity, such as backup management and disaster recovery, and crisis management

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures

(g) basic cyber hygiene practices and cybersecurity training

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption

(i) human resources security, access control policies and asset management

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

HOW CYBERSCOPE ADDRESSES SPECIFIC NIS2 MEASURES

CyberScope offers two key advantages to addressing NIS2 measures:

- The handheld form factor. By connecting directly to any perimeter physical port or wireless access point, this "see the edge from the edge" perspective provides a much more comprehensive view of potential cybersecurity vulnerabilities. Compared with centralized cybersecurity solutions, this makes it uniquely positioned to address several NIS2 measures at the network edge.
- The many capabilities associated with the CyberScope Cybersecurity Assessment Workflow (described below) can be efficiently implemented in a straightforward process that can subsequently serve as input into more extensive enterprise audits and compliance efforts.

[**] New rules to boost cybersecurity of EU's critical entities

[***] NIS2 Directive, Article 21: Cybersecurity risk-management measures (nis-2-directive.com)

CyberScope can aid in addressing aspects of NIS2 minimal obligations. Here is summary of where it can help:

CyberScope can aid in addressing aspects of NIS2 minimal obligations.

NIS2 Minimal Obligations	How CyberScope Addresses
Policies on risk analysis and information system security	Helps ensure visibility into organizational assets, a crucial part of managing risk Validates secure network configurations, which is part of risk management Supporting CyberScope features: • Endpoint & Network Discovery • Wi-Fi and Bluetooth/BLE Site Survey • Automated Discovery Monitoring • Automated Network Topology Mapping • AutoTest: DNS Validation • Wi-Fi Interference (DOS) Detection • AutoTest: VLAN ID, Monitoring, Device Reachability • Path Analysis • Rogue AP & Wireless Client Locate • Authorized Device List
Incident handling	Identifies vulnerabilities to respond to attacks, which ties into incident preparedness by aiding in the expedited restoration of services Supporting CyberScope features: • Integration of Nmap into AutoTest & Network Discovery • Standalone Nmap App • AirWISE® Automated Wi-Fi Security Problem Detection • AutoTest: VLAN ID, Monitoring, Device Reachability • Wi-Fi Interference (DOS) Detection
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Essential and important entities must continuously test cybersecurity controls in place via ongoing monitoring and the implementation of countermeasures in response to emerging or zero-day threats Supporting CyberScope features: • Endpoint & Network Discovery • AutoTest: VLAN ID, Monitoring, Device Reachability • Automated Discovery Monitoring • Wi-Fi Interference (DOS) Detection • AirWISE® Automated Wi-Fi Security Problem Detection • Authorized Device List

SUMMARY

Because of its distinct design, form factor, and capabilities, CyberScope, in conjunction with Link-Live, can aid your larger NIS2 compliance initiatives, mapping to key aspects of NIS2's minimal obligations. In the process, CyberScope greatly strengthens your organizations security posture while increasing overall situational awareness at the network perimeter.

APPENDIX

Below is more in-depth description of the minimal obligations of the NIS2 Directive Article 21, Cybersecurity risk-management measures.

NIS2 Minimal Obligations	Description/Summary
Policies on risk analysis and information system security	• Organizations must conduct regular risk assessments and establish robust information system security policies. This ensures that potential risks are identified, assessed, and mitigated in a timely manner. The policies must be reviewed and updated to address evolving threats and vulnerabilities • Risk assessments help organizations prioritize cybersecurity investments and implement protective measures that are aligned with the risks they face
Incident handling	• Organizations must develop procedures and protocols for detecting, managing, and responding to security incidents. This includes setting up incident response teams, establishing response protocols, and ensuring that incidents are reported both internally and to relevant authorities • Incident handling should ensure that damage is minimized, normal operations are restored quickly, and relevant stakeholders are kept informed
Business continuity, such as backup management and disaster recovery, and crisis management	• Businesses must create plans for maintaining operations in the event of a cybersecurity incident. This includes crisis management protocols that will guide decision-making during a cyberattack or major disruption • The goal is to ensure minimal interruption to essential services, enabling a quick return to normal operation after an incident
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	• The NIS2 Directive requires organizations to ensure that the third-party providers within their supply chain also adhere to robust cybersecurity practices. This could involve due diligence when selecting suppliers, regular security audits of third-party vendors, and contractual requirements related to cybersecurity • Companies must ensure that their vendors and service providers have sufficient cybersecurity measures in place
Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	• Cybersecurity must be embedded into the entire lifecycle of systems and software, from acquisition to development and ongoing maintenance. This means security features should be integrated at the design stage and continuously monitored for vulnerabilities • Regular patching, updates, and testing of systems and software must be implemented to mitigate security risks
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	• Organizations need to periodically evaluate the effectiveness of their cybersecurity controls and risk management strategies. This can include internal and external audits, continuous monitoring, and adjusting controls in response to newly identified vulnerabilities or threats • Testing and reviewing existing security measures ensure that the organization's cybersecurity framework remains robust and responsive to changes
Basic cyber hygiene practices and cybersecurity training	• Companies must promote basic cyber hygiene among employees and ensure that staff members receive cybersecurity training. This includes regular awareness campaigns on identifying phishing attempts, password management, and safe use of IT systems. • Employees must be equipped with knowledge on how to recognize and respond to potential cybersecurity threats.

NIS2 Minimal Obligations	Description/Summary
Policies and procedures regarding the use of cryptography and, where appropriate, encryption	• The directive mandates the use of appropriate cryptographic measures to protect sensitive information. Data encryption must be implemented for data both in transit and at rest to ensure confidentiality, integrity, and authenticity. • Encryption mechanisms should be applied to protect communications and stored data from unauthorized access.
Human resources security, access control policies and asset management	• The directive requires organizations to implement security measures regarding the hiring, training, and ongoing monitoring of employees with access to critical systems. This includes background checks, strict access controls, and role-based security privileges. • Human resource policies must ensure that employees with access to sensitive information or systems are trustworthy and adequately trained in cybersecurity practices.
The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	• Strict access controls must be implemented to ensure that only authorized personnel have access to critical information and systems. Organizations should adopt role-based access control, multi-factor authentication (MFA), and log access attempts. • These measures help prevent unauthorized access to sensitive data and systems, limiting the impact of potential security breaches.

USEFUL LINKS

NIS2 Directive Training, Updates, Compliance (nis-2-directive.com)

NIS2 Directive, Article 21: Cybersecurity risk-management measures (nis-2-directive.com)

NIS2 Requirements | 10 Minimum Measures to Address (nis2directive.eu)

What is NIS2? Get the Complete Picture (nis2directive.eu)

cyberscope.netally.com

netAlly
simplicity • visibility • collaboration