txOne networks

The OT Zero Trust Guide to Compliance with the NIS Regulations

Contents

1. The Background of the NIS Regulations

1.1 Introduction to the NIS Regulations

Every organization today uses interdependent cyber-physical systems that rely on software and networks to provide services in the physical world. However, when systems suffer from technical glitches, unintentional human error, or deliberate malicious attacks, it can severely impact the operators of essential services (OES) that we rely on in our daily lives, including electricity, transportation, water, energy, health, and digital infrastructure.

Any disruption to critical infrastructure affects social, security, and economic stability. To protect critical infrastructure in everyday life from cyber attacks, the European Commission proposed the Network and Information Security (NIS) Directive in 2016, the first EU-wide legislation related to cybersecurity, and Effective in 2018, May 9. Each EU member state must pass national legislation to follow or "transform" the Directive, and it will become law in the UK (2018), Belgium (2019), and others.

In the past, many companies might not think they would be targeted by hackers, resulting in limited cybersecurity awareness and investment. When EU member states adopt the basic security requirements common to the NIS Regulation, it helps keep cybersecurity on the agenda of board discussions. It ensures a minimum level of uniform security measures across EU member states. In addition, it is essential to improve the overall security level of essential services (OES) and digital service providers.

1.2 What are the NIS Regulations for

The NIS Directive sets three main goals:

1. National capabilities: EU Member States must have specific national cybersecurity capabilities in their respective EU countries (for instance, they must have a national CSIRT, conduct cyber exercises, and so on).
2. Cross-border cooperation: cross-border cooperation between EU countries (such as operating the EU CSIRT network and strategic NIS cooperation group).
3. National regulations in key sectors: EU member states must regulate the cybersecurity of their crucial market operators, which are ex-ante and ex-post supervisory regime in key sectors (energy, transport, water, health, digital infrastructure, and finance). These factors also apply to critical digital service providers (online marketplaces, cloud, and online search engines). For example:
    1) Ex-ante supervisory regime: OESes and DSPs should take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of the networks and information systems they use in their operations.[1]

[1] *The European Parliament and the Council of the European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union," July 19, 2016, articles 14.*

2) Ex-post supervisory regime: OES and DSPs must notify their competent authorities and/or national CSIRTs of any event that may disrupt their services. They must be notified of these events on time, a requirement similar to the GDPR.

1.3 Applicability of the NIS Regulations

The NIS Regulations' requirements for cybersecurity go beyond protecting personal data. They focus more on the availability, integrity, and confidentiality of systems and networks. Because the continued operation of OESes and DSPs is critical to organizations, and because both are mainly applied to critical infrastructure providers, the law is applied based on these two main types of organizations.

1. **Operators of Essential Services (OES):**

   The NIS Directive imposes legal obligations on operators of all essential services, including energy, banking, transport, water, health, financial markets, and digital infrastructure. Defining operators of essential services rests primarily with existing regulators in these sectors. Once identified as "Operators of Essential Services" (OES), these OESes must take appropriate and proportionate security controls to manage their risks to networks and information systems. Secondly, OES must notify relevant national authorities of serious incidents to ensure they "take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of the networks and information systems they use in their operations."

2. **Digital Service Provider (DSP):**

   An organization is a "Digital Service Provider" if it provides certain digital services. However, NIS does not apply to all digital services. To be covered, digital services must be one or more of the following: online search engines, online marketplaces, and cloud computing services. DSPs must self-register with their administration and determine if they are in-scope digital service providers. An excellent way to determine this is to ask yourself the impact on European countries if an organization ceased operations tomorrow:

   - Will there be a significant impact on the country?
   - Do you provide critical services to OES?

   Also, taking the UK as an example, the UK Information Commissioner's Office (ICO) provides some additional criteria to help organizations determine their suitability. If an organization meets these criteria, then the organization can be listed as a DSP and must comply with NIS requirements. DSPs are defined as follows:[2]

   - Provide one or more of the following digital services: online search engines, online marketplaces, and cloud computing services; or
   - Organization is headquartered in the UK or has appointed a UK representative.
   - Organization employs more than 50 employees and has a turnover or balance sheet of more than 10 million euros.

[2] *ICO of UK, "The Guide to NIS: What is NIS?", December 2021.*

2. Exploring the NCSC Cyber Assessment Framework (CAF)

The NIS directives primarily require organizations to achieve a certain level of security rather than provide specifics on how to implement them. As a result, many countries are thinking about how to apply specific technical measures to assist organizations in evaluating and implementing these regulations. The framework of most interest is the UK National Cybersecurity Centre (NCSC), which published the first version of the Cyber Assessment Framework (CAF) Guidelines in 2018. The CAF is a framework for assessing organizations covered by the EU Network and Information Systems Security (NIS) Directive and guides on how to practice it, including four pillars in total and 14 principles:[3]

Objectives	Principle	Description
A: Managing Security Risk	Governance	There are appropriate management policies and processes in place to govern the organization's approach to the security of network and information systems.
	Risk management	The organization takes appropriate steps to identify, assess and understand security risks to network and information systems supporting the delivery of essential services. This includes an overall organizational approach to risk management.
	Asset management	All systems and/or services that are required to maintain or support essential services are determined and understood. This includes data, people and systems as well as any supporting infrastructure (such as power or cooling).
	Supply chain	The organization understands and manages security risks to the network and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.

[3] *Jason G,"The Cyber Assessment Framework 3.1", The National Cyber Security Centre (NCSC), April 2022.*

Objectives	Principle	Description
B: Protecting Against Cyber Attack	Service protection policies and procedures	The organization defines and communicates appropriate policies and processes that direct the overall organizational approach to securing systems and data that support delivery of essential services.
	Identity and access control	The organization understands, documents and controls access to systems and functions supporting the delivery of essential services. Rights or access granted to specific users or functions should be understood and well managed. Users (or automated functions) that can access data or services are appropriately verified, authenticated, and authorized.
	Data security	The organization prevents unauthorized access to data whether through unauthorized access to user devices, interception of data in transit or accessing data that remaining in memory when technology is sent for repair or disposal.
	System security	Network and information systems and technology critical for the delivery of essential services are protected from cyber attack. This includes minimizing the opportunity for attack by configuring technology well, actively managing software vulnerabilities, minimizing services available, and controlling connectivity and physical access.
	Resilient networks and systems	The organization builds resilience against cyber attack and system failure into the design, implementation, operation, and management of systems that support the delivery of essential services.
	Staff awareness and training	Staff are given appropriate support to ensure they can support the security of network and information systems of essential services.
C: Detecting cybersecurity events	Security monitoring	The organization monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the on-going effectiveness of protective security measures.
	Proactive security event discovery	The organization detects anomalous events in the network and information systems affecting, or with the potential to affect, the delivery of essential services.

Objectives	Principle	Description
D: Minimizing the impact of cybersecurity	Incidents Response and recovery planning	There are well-defined and tested incident management processes in place that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities are in place that are designed to contain or limit the impact of compromise.
	Improvements	When an incident occurs, steps must be taken to understand the root cause of that incident and take appropriate remediating action.

3. Compliance with the NIS Regulation Requirements

TXOne Network is the leader in OT Zero Trust, and “Keeps the Operations Running all the time” enables the risk assessment process by providing visibility of the OT environment, policies, and trust list with cyber threat detection expertise.

1) **OT zero trust for inbound devices:**

   This cybersecurity policy takes effect from the moment a device comes onto your premises. Newly-arrived assets being prepared for onboarding should also be pre-scanned (*Trend Micro Portable Security 3*) to mitigate the risk of supply chain attack – in the past, cyber attackers have triggered cyber incidents by compromising devices prior to shipment.

2) **OT zero trust for appliances:**

   Traditional antivirus software can bog down assets, leading to crashes or delays. Operations-friendly, “OT-native” lockdown software (*StellarEnforce*) secures legacy endpoints with a trust list that only allows applications critical to operations. For modernized endpoints that carry out more varied or complex tasks, a library of trusted ICS applications and licenses informs next-generation antivirus software (*StellarProtect*) as to which files and applications it can skip and give priority to, preserving resources for operations.

3) **OT zero trust for networks:**

   Attackers find your OT network much more challenging to attack when unnecessary “doors” in the network are sealed with specific rules for traffic put in place by firewall or IPS appliances (*EdgeIPS* & *EdgeFire*). With these special rules for traffic, which are based strictly on which assets need to communicate to do their work, the network is separated into segments that are easier to monitor and secure. For legacy and otherwise unpatchable assets, virtual patching shields vulnerabilities so

that they cannot be exploited by attackers. Network appliances and policy are easily observed and maintained through a single, centralized console (*OT Defense Console*).

3.1 Objective A: Managing Security Risk

Find below the recommended organizational structures, policies, and processes necessary to understand, assess, and systematically manage security risks to networks and information systems supporting essential services.

Principles under the Objective A include:

Objective A	Evidence of Compliance	TXOne Products
Governance	• OT cybersecurity policy • Responsible, accountable, consulted, and informed (RACI) charts • KPIs and senior management buy-in • Risk assessment process	• The ODC (*OT Defense Console*) platform enables centralized management of cyber defense provided by *Edge* series nodes, even when nodes are distributed across multiple work sites. • *StellarProtect* & *StellarEnforce* lock down modernized and legacy assets running side-by-side and allow management from a single pane of glass via *StellarOne*. • *Trend Micro Portable Security 3* creates an inventory of OT asset information during routine scans, allowing verification of vulnerability status, version information, and compliance with regulations.
Risk Management	• Risk assessment records • Industrial automated control system drawing(s) • Risk assessment review records and improvement management plan	• *Trend Micro Portable Security 3* generates an inventory for all scanned assets that allows confirmation of vulnerability and risk status.
Asset Management	• Simple industrial automated control system network drawing(s) • Asset inventories • Plan for aging and obsolete hardware and software	• Scan assets with *Trend Micro Portable Security 3* before onboarding, enabling stakeholders to confirm digital hygiene while also tracking asset security status through the entire asset life cycle.

Objective A	Evidence of Compliance	TXOne Products
Supply Chain	• List of roles and responsibilities for involved third parties • Definition of cybersecurity requirements for third parties • Reports of completed assessment and assurances from third parties	• Scan every OT asset or device that comes onto the work site for regulatory compliance with *Trend Micro Portable Security 3*, including service vendors' and contractors' laptops. • Use *Trend Micro Portable Security 3's* asset scan logs create an "OT health check", or a record of digital hygiene for both internal and external use that helps organizations create a secure supply chain

3.2 Objective B: Protecting Against Cyber Attacks

Proportionate security measures in place to protect essential services and systems from cyber attack or system failures.

The Principles under the Objective B include:

Objective B	Evidence of Compliance	TXOne Products
Service Protection Policies and Procedures	• Published and controlled policies, procedures, work instructions, etc. • Personnel security records (recognizing data protection requirements) • Configuration records (e.g. for firewalls, etc.) • Management of change records • Organizational and procedural change control records • Validation test records • Audit reports, review reports and management of resulting actions	• Use *OT Defense Console* to manage the policies and processes of networking and endpoint security assets, enabling stakeholders to secure operational integrity even between separate, geographically distant work sites. • Implement *Trend Micro Portable Security 3* in the work site's cybersecurity plan to mitigate the risk of malicious code landing with asset scans and asset inventories that include stand-alone and air-gapped as well as networked assets.

Objective B	Evidence of Compliance	TXOne Products
Identity and Access Control	• Authentication and authorization • Records of current authorized users, assets, and the level of access or privilege, etc. (noting data security requirements) • Records of change management for users, control of physical tokens or cards, etc. • Records of physical access control authorization and physical access control measures, e.g. key distribution or electronic access control records	• Use business intention to model routine tasks and network traffic, then make rules for intra- and inter-segment traffic with *Edge* series products. • Use *Trend Micro Portable Security 3* to periodically scan OT assets and service vendors' or contractors' laptops for regulatory compliance. Conduct scans of incoming and outgoing devices for both insider threat elimination and supply chain security purposes.
Data Security	• Relevant procedures for identification of sensitive data, assets containing this data, and how they are protected • Specification of encryption algorithms and keys used • Records of essential data, services, and connections identified and how these are protected where required	• Deploy *EdgeIPS* & *EdgeFire* to segment the network based on understanding of regulations, data sensitivity requirements, and work group productivity – this prevents attackers from moving within your network or accessing any sensitive devices. • Apply *Edge* series network-based virtual patch technology to create a shield around legacy OS or unpatched assets that prevents attackers from exploiting a vulnerability to access sensitive data. • Define roles using trust list-based lockdown software *Stellar* to secure mission critical systems data against disruption. • *Trend Micro Portable Security 3* scans sensitive air-gapped or standalone assets that sometimes cannot accept installations or even light modifications, creating an inventory of them and assuring they are threat-free while still adhering to their sensitivity needs. • *Trend Micro Portable Security 3 Pro* includes secure storage equipped with AES-256 encryption to completely safeguard file transfer in your work site.

Objective B	Evidence of Compliance	TXOne Products
System Security	• Procedures setting out requirements for network architecture, segregation and access • IACS simple network drawings • Asset hardening procedures, instructions, templates, vulnerabilities, and threat records • Patch management procedures and records, as well as records of associated change management	• Conduct system hardening with the *Stellar* series lockdown software – use machine learning and trust lists to prevent all unapproved or suspicious applications and operations. • *Edge* series virtual patching addresses even unpatchable asset vulnerabilities at a network level without requiring any re-configuration or changes to the asset being secured. • Streamline management and reference of records with the inventory of scanned assets automatically created by *Trend Micro Portable Security 3's* scan process.
Resilient Networks and Systems	• Records of review of limitations, constraints, and weaknesses • Disaster recovery strategy Software / firmware / application / configuration libraries and safes • Restoration test records	• Segment networks with the *Edge* series to make OT environments inherently more defensible, preventing lateral movement and other malicious actions by hackers • Use *Edge* series appliances to create special rules for traffic which are based strictly on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity. • The *Stellar* series prevents unapproved USB device connectivity, script execution, and changes to configurations or data.
Staff Awareness and Training	• Definition of competence requirements for defined IACS roles and responsibilities • Cybersecurity awareness training program • Competence management records	• OT zero trust-based solutions increase the efficiency of cybersecurity planning and execution, enabling more economical manpower requirements while streamlining oversight and management concerns. • *Trend Micro Portable Security 3* is an easy-operation scan device, requiring no special training or education to use.

3.3 Objective C: Detecting Cybersecurity Incidents

Appropriate capabilities to ensure network and information system security defenses remain effective and to detect cybersecurity events affecting, or with the potential to affect, essential services.

The Principles under this Objective C include:

Objective C	Evidence of Compliance	TXOne Products
Security Monitoring	• Procedures setting out security monitoring requirements including malicious code detection • Records of periodic monitoring (e.g. of security logs, virus detection logs, intrusion detection logs etc.) • Analysis and interpretation of the threat intelligence, periodic monitoring records, and management of resulting actions	• Network segmentation with the *Edge* series streamlines monitoring and inspection of OT traffic, even when specialized ICS protocols are in use. • *Trend Micro Portable Security 3* creates centrally recorded asset inventories during every scan.
Proactive Security Event Discovery	• Relevant proactive security event discovery procedures • Analysis and interpretation of associated test and / or monitoring records and management of resulting actions	• Network segmentation with the *Edge* series brings unusual or suspicious activity directly to the attention of stakeholders on a need-to-know basis to prevent alert fatigue. • Identify and remove any malware brought onto enterprise assets by third parties via *Trend Micro Portable Security 3*, and use security records to get to the root of any recurring issues quickly. • *Stellar* disallows all activities that are not specifically trust listed while providing threat detection, including machine learning that identifies suspicious or malicious actions that are often part of unknown attacks.

3.4 Objective D: Minimizing Impact of Security Incidents

Capabilities to minimize the impacts of a cybersecurity incident on the delivery of essential services including the restoration of those services where necessary.

The Principles under this Objective D include:

Objective D	Evidence of Compliance	TXOne Products
Incident Response and Recovery Planning	• Incident response plan • Incident response exercise plans and records	• Use *Trend Micro Portable Security 3's* threat detection and quarantine functions to stakeholders to identify, analyze and initiate a strategic response to a cybersecurity incident. • Detailed scan logs and reports from TXOne solutions allow you to understand the target, nature, and potential impact of a threat. Determine the appropriate amount of time to retain logs based on your needs. • Scan logs can also be exported to CSV files and then stored as evidence for nonrepudiation purposes or transferred to an SIEM (such as QRadar or Splunk) or Rsyslog server.
Improvements	• Post-incident and post-exercise root cause analysis • Improvement management plan • Evidence of review of incident response plans	• Conduct precise forensics with highly detailed scan logs and reports generated by the *Edge* series, the *Stellar* series, and *Trend Micro Portable Security 3*.

4. Conclusion

The NIS Regulations are critical to creating a higher standard of cyber defense capable of resisting potentially catastrophic modern cyber attacks. A prevention-based cybersecurity strategy is not enough, and companies must instead build resilience into their work sites by implementing security controls and rapid response. It is recommended that OES and DSP organizations need to take appropriate and proportionate technical and organizational measures to manage both IT and OT risks. The cases of the Solar Winds supply chain compromise (December 2020) and the attack on a well-known pipeline company (May 2021) show that there are still a few common ways in which organizations could pay more attention to OT cybersecurity and their supply chain cybersecurity risks, thus better protecting their bottom line. Streamline compliance with the NIS Regulations using TXOne's OT zero trust-based solutions to custom-generate OT-native, naturally defensible security policies that ensure operational integrity, secure the supply chain against attack, and keep the operation running.

txone.com