FORESCOUT

NIS

No Time to Lose: How to Help Ensure Your ICS Infrastructure Complies with the EU's NIS Directive

Executive Summary

In today's increasingly digital world, the IT infrastructures supporting the provision of essential services are becoming more complex and critical to effective operations. This also makes them more vulnerable to attack and failure.

The EU's Directive on the security of network and information systems (NIS), establishes an advanced set of cyber security objectives for organizations supplying essential services in the EU.

For essential service providers, non-compliance is not an option, since breaches of the Directive could generate significant fines in the millions of Euros. However, the definition of what constitutes an essential service, and how the NIS will be applied, is different in every EU country.

This eBook explains the NIS Directive and its implications for essential service providers that depend on ICS networks to operate effectively. It also defines how essential service providers should assess solutions designed to support NIS compliance, and describes how ForeScout Technologies' approach helps organizations meet the requirements of the Directive.

Introduction

Increasingly, essential services in our society rely on digital ICS infrastructures to function. They control the operation of everything from power grids to emergency response. This makes cyber threats more dangerous than ever, because the potential consequences of insufficient ICS protection go beyond damage or loss of data, to include major disruption to our lives.

Not only that, the complexity caused by the increasing connectedness of ICS environments increases risks further. For example, a more complex environment increases:

- The number of potential entry points for cyber adversaries
- The likelihood of unplanned downtime
- The cost and effort involved in managing the converged environment
- The number and diversity of people involved in defining and ensuring the security the environment
- The difficulty of ensuring compliance

To mitigate risks and ensure service availability, the NIS Directive establishes an advanced set of cyber security objectives for organizations supplying essential services in the EU. The Directive came into force in May 2018 but is being applied differently within countries based on their own definitions of essential services.

Ensuring compliance is urgent for any organization operating in Europe because failure to comply could generate millions of Euros in penalties. Since ICS are central to the infrastructures of all organizations supplying essential services, securing them in a NIS-compliant manner must be a priority.

However, essential service providers need to use the right approach and technologies to secure their ICS. Otherwise, they risk exposing themselves to the financial risks of both cyberthreats and compliance failures.

“Since ICS are central to the infrastructures of all organizations supplying essential services, securing them in a NIS-compliant manner must be a priority.”

What Is the NIS Directive?

The NIS Directive is designed to help prevent societal disruption in Europe by ensuring the providers of essential services are properly protected against cybersecurity threats. Specifically, the objective is to significantly increase the resilience of the ICS networks that support the provision of those services. To this end, the Directive makes recommendations about how organizations should:

- Approach security assessment and risk management
- Manage the operational impact of cyberattacks
- Share information about security incidents
- Train people to properly implement protection measures.

NIS Compliance Overview[1]

Factor	NIS
Incident Reporting	Required when substantial impact on essential services occurs
Maximum Potential Fine	To be determined by country governments e.g. the UK has defined a maximum flat rate fine of GBP 17 million [2]
Double counting of incidents (the same incident can be fined under both NIS and GDPR)	Yes

When and How Is the NIS Directive Being Implemented?

Although the Directive came into force in May 2018, national governments within the EU have been given until November 2018 to provide their own definitions of essential services. Based on those specific definitions, the implementation of regulations will vary between individual countries.

> "The financial penalty for NIS non-compliance in the UK has been set at a flat rate of GBP 17 million."

What Is an Essential Services Provider? [1]

The final definition will vary in every country, but there are 3 key criteria that will guide the selection of the providers that are affected:

- Provides a service that is essential to the normal functioning of society
- The effective provision of that service depends on IT/OT networks and information systems
- Any incident which affects the operation of the service would have a severely disruptive effective on society

Roadmap to NIS

- March 2013: Negotiation by Council of EU member states and the European Parliament begins
- May 2015: NIS Directive approved by the Council
- July 2015: NIS Directive approved by the European Parliament
- December 2015: European Parliament and Council Agreement
- 2016: NIS Directive transposition into national legal frameworks
- May 10th 2018: NIS Directive comes into force
- November 2018: Deadline for countries to define essential service providers

Utilities, gas suppliers, transport companies and many others are affected by the NIS Directive and must start preparing to comply with the regulations, as defined by the relevant authorities within the countries in which they operate.

How Does the NIS Directive Impact ICS Security?

ICS networks are a central element of essential service provider infrastructure. That's why protecting these networks must become a priority for any organization that needs to ensure NIS compliance. ICS asset owners within these organizations must now:

- Secure the systems and facilities used for the provision of essential services (including ICS)
- Monitor both IT and OT networks with comprehensive threat detection systems
- Demonstrate mature incident management and remediation protocol
- Implement effective and accurate incident reporting mechanisms

These tasks are made all the more difficult by the increased IT/OT complexity described above. Nevertheless, the NIS Directive was designed to ensure that essential service providers remain responsible, accountable and educated on evolving cyberthreats that can affect economies and people. And because the cyberthreat landscape is always evolving, the NIS Directive is likely to evolve as well. To keep up with these changes and new threats as they occur, selecting and investing in the right cybersecurity tools will be an important strategic business decision.

"To keep up with these changes and new threats as they occur, selecting and investing in the right cybersecurity tools will be an important strategic business decision ."

These are a few of the capabilities that essential service providers should carefully assess when selecting any IT or OT cybersecurity solution:

1. Comprehensive and optimized threat detection capability
2. Support for workflow integration and real-time incident management
3. Detailed asset inventory and reporting
4. Ability to report and provide evidence of security policy implementation
5. Ability to track and manage security audit results

Best Practices for Approaching NIS Compliance

Existing best practices for protecting ICS networks provide a good foundation for addressing the NIS Directive's requirements. These include: the US ICS-CERT Defense-in-Depth; US NERC CIP ESP (Electronic Security Perimeter) access control; Gartner's guidelines for OT security; the ISA Purdue model of control; and ISA99/IEC62443.

Nevertheless, each country is responsible for defining its own requirements for ensuring that essential service providers comply with the NIS Directive. As an example, we have looked at the NIS compliance requirements defined by the UK's National Cyber Security Centre, part of the GCHQ (Government Communications Headquarters), and defined how ForeScout Technologies approaches the protection of essential service provider infrastructure in relation to each of them[3]. This information is summarized on the next page.

ForeScout Technologies' Approach to Key NISD Principles

Principle	Requirement	ForeScout Technologies Approach
Governance	Governance structures, policies and practices must be clearly defined. A single individual (or group) should hold overall responsibility and accountability for deciding how to protect services and ensure security. Governance structure sophistication should reflect the size and resources of the organization.	SilentDefense helps to clearly identify the system under consideration, including security perimeter definition and access point identification. SilentDefense automatically generates and visualizes an inventory of all active network devices and communications. It then presents it to the user in the form of an interactive network map and clear network baselines. This enables users to: • At the design stage, identify the current (or define the intended) security perimeter and access points (e.g. gateways, firewalls, etc.). • At enforcement time, ensure that all communications accessing a network and its devices pass via the intended access points. Real-time alerts flag communications which violate flow and perimeter restrictions.
Risk Management	Security risks vary widely among industries and organizations. Every essential service provider must have systematic processes in place to adequately identify and manage the risks most relevant to their situation.	SilentDefense accelerates the risk assessment process for service providers. Dedicated libraries help identify system vulnerabilities and detect ICS-specific threats and flaws. They also enable accurate analysis and reporting of all the active devices and services in a network.

Principle	Requirement	ForeScout Technologies Approach
Asset Management	A deep understanding of service dependencies across hardware, software, data, staff and associated networks is required to accurately identify and address risks. Clear documentation is required to ensure it is easy to understand which elements are crucial to essential service delivery and why.	SilentDefense automatically determines the control system role for each device on the network, and provides asset inventory information such as model number, firmware version, and serial number if available within the network protocols. The solution also provides comprehensive reporting.
Supply Chain	Essential service providers are responsible for service delivery and the associated security requirements, even if delivery requires third-party involvement. Contracts with third-parties must ensure the protection of all the elements required for essential service provision.	SilentDefense enables field device access monitoring, alerting, and reporting on authorized or unauthorized activities, helping to ensure operational and business policies are upheld.
Service Protection Policies & Processes	Comprehensive security policies and associated processes must be defined and implemented within the infrastructures of all essential service providers. These must be available in versions that are understandable to both technical and business audiences. Validation mechanisms should also be in place to ensure policies and processes are being upheld. However, policies and processes must be realistic so that users do not resort to insecure workarounds.	SilentDefense can play a major role in defining communication baselines for all devices and assets in control system environments. In addition, SilentDefense logs and provides alerts about changes to firmware or hardware versions.

Principle	Requirement	ForeScout Technologies Approach
Identity & Access Control	Authentication and authorization of users, devices and systems must be assured before access to data or services is granted. This may require the implementation of two-factor or hardware authentication, so that unauthorized individuals cannot gain access.	SilentDefense provides visibility and situational awareness over network devices and communications. It tracks and logs all successful and failed authentication attempts to network resources. Access to the information gathered by SilentDefense can be restricted to authorized users.
Data Security	Data protection coverage must be aligned with the risks of data being compromised. This may also involve the sanitization of the physical media used to access or handle that data. Risks to essential service delivery caused when data integrity or availability is compromised in situ or in transit must also be addressed. Any OES relevant information that could help attackers carry out a successful attack must be identified and properly protected.	SilentDefense allows proactive identification of firmware versions that are not up to date compliant with corporate policy. SilentDefense also reports any undesired network communication and activity, helping to ensure ing that network integrity and segregation is preserved. Finally, SilentDefense enables users to verify that sensitive information is communicated using secure encrypted protocols and cipher suites.

Principle	Requirement	ForeScout Technologies Approach
System Security	Every essential services provider is responsible for applying security measures that are most appropriate for the specific risks that they face. Vulnerabilities caused by flaws, features and user error must all be addressed using these measures. Software vulnerabilities in particular should be avoided through regular updates and patching. Limiting functionality can be an important part of eliminating feature-centric vulnerabilities. Staff training is also an important element in preventing vulnerabilities caused by human error, such as accidentally revealing sensitive data.	Essential service providers can use SilentDefense to accelerate their OT risk assessment processes. Industrial Threat Library (ITL) allows instant detection of known vulnerabilities along with ICS-specific threats and flaws from security, network, and operational perspectives. In conjunction with reporting and API features, SilentDefense provides quick, automated report generation.
Resilient Networks & Systems	Regular maintenance is essential for proper protection, and admin interfaces in particular must be well protected. Limiting the use of management accounts for conducting day-to-day activities such as web browsing limits the number of potential access points for hackers.	SilentDefense provides real-time visibility into all network communications, allowing essential service providers to harden their network access controls and ensure least privilege.

Principle	Requirement	ForeScout Technologies Approach
Staff Awareness & Training	Staff are often the weakest link in the security chain, so they must have access to the knowledge and skills they need to uphold security. Crucially, the information they receive must be tailored to the realities of their day-to-day work.	The ForeScout Technologies Academy provides our partners and clients with the knowledge and tools to get certified in OT security with the ForeScout Technologies solution.
Security Monitoring	Proper monitoring that really analyzes what is happening within the infrastructure and enables a timely response to any issues that are detected is essential. Threats are changing and evolving continuously, so security measures must reflect this and provide adaptable, ongoing protection.	SilentDefense is a continuous network security monitoring technology designed specifically to identify security events in industrial control systems. As such, it can outline which specific types of threats and anomalies are being identified and send them to various stakeholders (IS, network, OT). SilentDefense also supports physical security and building automation and control protocols and security event detection.
Anomaly Detection	Security systems must be able to proactively detect indirect indicators of threats or suspicious activity, beyond those direct indicators recognized by standard security solutions. These indicators will vary between service providers, but must be accommodated, whatever form they take.	SilentDefense can automatically create both network and protocol baselines for ICS environments. These help to ensure all communications happening within the control system are known and approved communications working in the manner they have been designed and engineered for.

Principle	Requirement	ForeScout Technologies Approach
Response & Recovery Planning	100% security is never achievable and, when incidents occur, essential service providers must have mechanisms in place to minimize their impact on service provision. These mechanisms may include system redundancy, automated backup or manual failover processes.	The SilentDefense network and protocol baselines can be used in recovery situations to help ensure devices and applications are operating as expected.
Improvements	Essential service providers must ensure why an incident occurred and take steps to ensure it cannot happen again. This means identifying and addressing the root cause, not the symptom.	SilentDefense alerts provide rich contextual information about the source, nature and target of threats, along with key input for analysis (including packet capture related to the threat). Together with the ability to visually locate each threat and its spread on the interactive network map, the information contained in alerts is fundamental to initiate an effective incident response process.

Conclusion

Complying with the NIS Directive as it applies in specific countries of operation is an urgent requirement for any organization operating an ICS network in Europe. Failing to meet the requirements of the Directive represents a serious business risk that could cost millions. Existing best practices are a good starting point for meeting NIS requirements. However, an optimized, non-intrusive network monitoring and situational awareness platform for industrial networks is a best practice approach for addressing the key NIS Directive Security Principles.

Sources

[1] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[2] “Protecting our critical infrastructure: Understanding new cyber security laws” – Dr. Richard Piggin, Principal Operational Technology Cyber Security Consultant, Atkins
[3] https://www.ncsc.gov.uk/guidance/nis-directive-top-level-objectives

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com