POINT OF VIEW

6,5,4,3,2,1: The NIS2 Countdown Has Begun

6 Key Steps to Build a Mature NIS2 Program

The EU's Network and Information Security (NIS2) directive is almost here. Affected entities should be preparing for NIS2 compliance before October 17, 2024, the date EU nations must enact NIS2 implementing laws.

Some critical infrastructure operators affected by the 2016 NIS1 directive have mature NIS2 programs. But NIS2 affects tens of thousands more small and medium organizations that must gain management support for a NIS2 program, engage IT and operational technology (OT) security professionals and draft implementation plans. These steps will minimize compliance risks.

But what does a mature NIS2 program look like and why should you create one?

The threat environment in 2024 is much more sophisticated than 2016. Cyberattacks on Ukraine energy firms have endangered lives. Wiper malware on Viasat modems in February 2022[1] cut communications to 5,800 wind turbines in Germany. State-backed threat actors are using dormant accounts[2] to bypass cloud providers' access controls.

NIS2 requires all mid-sized and large organizations providing important and essential services to raise their guard, implement risk management for IT and OT environments, take ownership of supplier risks, be able to detect, respond to and recover from security incidents, and to swiftly report incidents.

EU countries preliminary drafts NIS2 law[3] show how countries may implement broader laws than the directive requires. In the case of Germany, the Federal Office for Information Security (BSI) can check compliance at its discretion, request evidence of risk management measures, and impose remediation orders.

NIS2 specifies laws that, at a minimum, require organizations to "take appropriate and proportionate technical, operational and organizational measures" to manage cybersecurity "appropriate to the risks posed". It's not prescriptive, but says organizations should follow EU and international standards, such as the ISO 27000 series for IT and IEC 62443 for OT.

[1] An Overview of the Increasing Wiper Malware Threat

[2] SVR cyber actors adapt tactics for initial cloud access

[3] Discussion paper from the Federal Ministry of the Interior and Homeland on NIS2 implementation

6 Key Steps to Build a Mature NIS2 Program

1. Do More Than Identify Security Risks

At a minimum, identify the risks and impact of disruptive cyberattacks on IT systems. A mature NIS2 program will also evaluate the severity of impacts on IT and OT environments, finances, human safety, operating capability when systems are down, environmental impacts, investor reactions, and how it affects the community and businesses.

This is enabled by establishing an accurate asset inventory. Organizations need to identify all network and information systems that are critical for business operations including hardware, software, data and any other digital asset.

This offers a clearer picture of the consequences of an attack, what's at stake, how to respond, how much it costs to remediate and recover, and what mitigations should be in place to prevent a repeat.

Evaluate the severity of different attack types on assets. Wiper malware on an OT environment that impacts safety is very different to a compromised engineering workstation. The evaluation and risk scores should be documented in a "risk register" like the one below. This will help you make decisions about how to manage assets and supply relationships impacted by NIS2.

Organizations need to identify all network and information systems that are critical for business operations including hardware, software, data and any other digital asset.

Table 2. Example of an NIS2 Cyber-Risk Register[9]

ID	PRIORITY	RISK DESCRIPTION	RISK CATEGORY	INDUSTRIAL CYBER RISK EVALUATION						RISK RESPONSE	COST/ BENEFIT ANALYSIS	RISK OWNER	STATUS
				FINANCIAL IMPACT	SAFETY IMPACT	BUSINESS CONTINUITY	ENVIRONMENTAL IMPACT	REPUTATIONAL IMPACT	NATIONAL IMPACT				
1	Very High	An advanced threat activity group targets our safety systems, leading to complete plant shutdown and associated property damage.	**Cyber Incident:** Loss of Safety	$70.5M	M	M	L	M	L	Install additional OT monitoring at the plant. Increase operator training for incident response and recovery.	**$350k** for monitoring & training.	Plant Management	Open
2	Moderate	ICS vendor is compromised, resulting in malware sent to all field devices in the form of a "legitimate" software update.	**Cyber Incident:** Supply Chain Compromise	$1.2M	M	M	L	M	M	Include procurement language for supply chain risk. Add technical evaluation to all patch management cycles.	**$50k** for insurance & an additional $150k for new patch management and supply chain recommendations	OT Security Team	Open
3	Low	Operator uses infected USB to transfer project files across plant operations. Untargeted malware causes network latency issues.	**Cyber Incident:** Engineering Workstation Compromise	$750k	L	L	L	L	L	Limit ports and services across Level 3 and Level 2 assets, including physical ports. Include additional security awareness for plant personnel.	**$25k** in hourly work to create OT-based strategy for plant operations and USB protections.	Plant Management	Open

Source: Enabling NIS2 Directive Compliance with Fortinet for Operational Technology

2. Security Posture Evaluation

Take responsibility for cyber risks and identify steps to improve security posture. Continuously assess, evaluate, improve and monitor your security posture and keep track of configurations and vulnerability remediation.

This is time-consuming work, but it matters and should be automated where possible. The DarkSide ransomware gang broke into Colonial Pipeline's OT environment[4] by using a dormant virtual private network (VPN) account. It should have been disabled.

According to a NSA and CISA[5] assessment, the two most common misconfigurations were software with default configurations and failing to separate user and administrator privileges.

Improve security posture by removing all default credentials and hardening configurations; disabling unused services and implementing access controls; updating software regularly and automating patching; and limiting and monitoring administrative accounts and privileges as well as auditing external surface areas subject to attacks.

The two most common misconfigurations are software with default configurations and failing to separate user and administrator privileges.

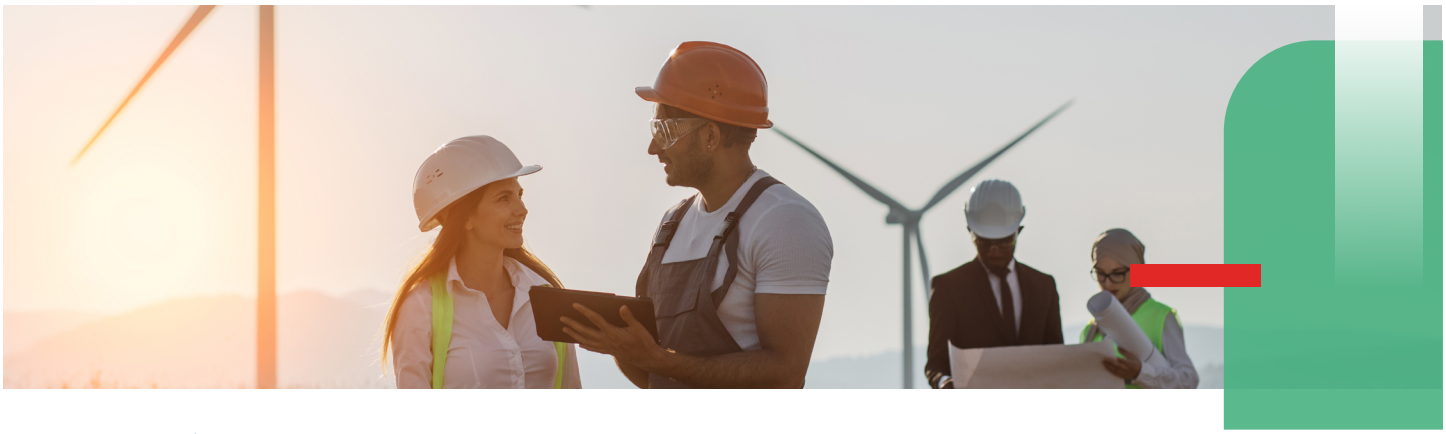
3. Scrutinize and Secure the Supply Chain

Modern economies are interconnected. Critical supply chains need to be protected. NIS2 aims to normalize the insufficient cyber resilience across businesses and Member States and developing a common understanding of the main vulnerabilities found in the Supply Chain. NIS2 aims to reduce supply chain security risks in software products, managed service providers and devices – from 5G base stations to ICS, remote terminal units (RTUs), SCADA, and the Internet of Things (IoT).

A mature NIS2 program accounts for all dimensions of supply chain risk. Identify important suppliers, original equipment manufacturers (OEMs), and IT and OT vendors and integrators. If suppliers appear in the risk register, adjust contract terms to account for supplier security posture, impact on their relationship and incident response due coordination.

Secure-by-design is gaining traction across the globe. It places greater onus on technology vendors to take ownership of customer outcomes and ensure solutions are inherently robust and not allowing that security technology arrives after the solutions have been deployed. The UK Ministry of Defence now includes secure-by-design in its supplier contracts[6]. In October 2023[7], cybersecurity agencies in 17 countries backed CISA's Secure By Design proposal.

Fortinet fully supports global adoption of secure-by-design[8] and secure-by-default, which are core to the Fortinet Secure Product Development Lifecycle (SDLC) policy[9] for all products, components, and services. We believe all security vendors should commit to the principle.



[4] Protecting Critical Infrastructure: Colonial Pipeline, DarkSide, and Ransomware

[5] NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

[6] Ministry of Defence: Industry Security Notice

[7] CISA, U.S. and International Partners Announce Updated Secure by Design Principles Joint Guide

[8] Three Keys to Secure-by-Design Implementation

[9] Fortinet Secure Product Development Lifecycle

4. Streamline Incident Reporting

Nominate a dedicated responsible person for incident reporting and have processes for effective coordination and response. Entities must submit an early warning of a significant incident to their designated Computer Security Incident Response Team (CSIRT) or competent authority without undue delay and, in any event, within 24 hours of becoming aware of the incident. This is followed by an incident notification within 72 hours, providing an initial assessment of the incident, including its severity and impact. Finally, a detailed final report must be submitted no later than one month after the initial incident notification. A mature NIS2 program has processes to swiftly evaluate these factors and quickly assess if the incident was caused by malicious actors. Entities within the electricity sector should also align to EU Network Code on Cybersecurity, to assess whether it is likely to have a cross-border impact.

Organizations have 24 hours to report significant cyber incidents and must update the report with a severity and impact evaluation.

The European Commission has recently adopted the first-ever EU network code on cybersecurity for the electricity sector (C/2024/1383). Foreseen under the Electricity Regulation (EU) 2019/943 (Article 59) and in the 2022 EU Action Plan to digitalise the energy system, this delegated act is an important step to improve the cyber resilience of critical EU energy infrastructure and services.[10]

This network code establishes a governance model that uses and is aligned with existing mechanisms established in horizontal EU legislation, notably NIS2. This is the case, for example, for the reporting of cyberattacks and vulnerabilities using the established Computer Security Incident Response Teams (CSIRTs), or coordination with the CyCLONe network in case of large-scale cybersecurity incidents and crises.

[10] COMMISSION DELEGATED REGULATION (EU) .../... of 11.3.2024

5. Fortify Defenses Against Ransomware

According to Denmark's SektorCERT[11], all 48 cyberattacks that actually compromised networks of European energy and utilities companies since 2015 started with compromised IT. Fifteen of the attacks affected OT networks and 31 were ransomware attacks, 13 of which resulted in stolen data. Ransomware attacks that affect critical infrastructure suggests the sector isn't sufficiently separating IT networks from OT networks.

A mature NIS2 program encompasses people, processes, and technology. Prepare and educate employees and management with the knowledge that ransomware often starts with phishing. Attackers target IT networks and move laterally to OT, which makes network segmentation critical. Look for systems, such as Active Directory, that are on both OT and IT networks. Avoid direct remote access to systems on the OT networks and use multi-factor authentication (MFA) for remote access to IT and OT. Deploy honeypots in the OT network and monitor OT network traffic. And back up SCADA, PLC, RTU project files and configurations.

6. Work Towards a Zero Trust Architecture

The NIS2 Directive advocates enhanced security requirements aligned with the Zero Trust approach[12] which assumes no one inside or outside the network should be trusted unless their identity has been verified. Protect data, applications, assets, and services. A mature security organization will implement network micro-segmentation to thwart lateral movement. ZTNA is a secure replacement for legacy VPNs.

Fortinet recognizes that cybersecurity requires a collaborative effort and a holistic approach. We can help you develop a mature NIS2 program that helps you achieve compliance and improve your security capabilities.

Discover more information here

[11] Cyberattacks against European energy & utility companies

[12] Fortinet: What is Zero Trust?

FORTINET

www.fortinet.com

April 4, 2024 10:49 AM

2626554-0-0-EN