POINT OF VIEW

# Why Utilities Must Be Ready for the Impact of NIS2

## The European Union's (EU) New Network and Information Systems 2 (NIS2) Directive has Far-Reaching Implications for Energy Sector and Utilities.

The NIS2 directive was approved by the EU Council in November 2022 and gives member states until October 2024 to transpose NIS2 into national law to ensure its critical infrastructure sectors are in compliance.[1] However, reaching cybersecurity compliance for utilities requires long cybersecurity programs that necessitate an early start.

Utilities must get ahead of the NIS2 directive, which imposes stricter risk management, as well as incident response and incident reporting obligations on operators of essential services (OESs) than its predecessor, NIS. It also introduces tighter supervisory measures, stricter enforcement requirements, and harmonized sanctions across the EU, which affect electricity generation and distribution, oil and gas, air, rail, road, drinking water, and wastewater.

NIS2 comes at a time of sustained geopolitical tensions that have exposed critical infrastructure to a higher volume of attacks by advanced and state-sponsored attackers. In this sense, NIS2 is both a regulatory upgrade and an opportunity to invest in more resilient cybersecurity from every angle—people, processes, and technology.

The EU developed NIS2 to encourage critical infrastructure OESs to invest more in cybersecurity to mitigate costly disruptions caused by ransomware and supply chain attacks. These can affect the availability and integrity of cross-border critical infrastructure operations.

Additionally, many utilities have modernized their digital systems by deploying Industrial Internet of Things (IIoT) and new wireless technologies, including 5G, alongside converged IT and operational technology (OT) environments. These additions are increasing the cyber risk to critical infrastructures.

While the IIoT delivers cost savings through improved automation, analytics, and management, it also creates new attack surfaces. For example, Covid-19 pandemic restrictions caused many operators to introduce new technologies to support remote access to Industrial Control Systems (ICS) and OT environments. Air-gapped OT environments are also exposed by the need to interface with PCs and removable media to deliver updates and for command and control purposes.

Under NIS2, IT and OT—such as programmable logic controllers (PLCs), distributed control systems (DCSs), and human-machine interfaces (HMIs)—must be adequately protected. NIS2 doesn't prescribe what utilities should achieve but each entity must examine its own cyber risks and identify steps to improve security posture. NIS2 also encourages the adoption of key industry cybersecurity standards, such as ISA/IEC 62443 and ISO/IEC 27001.

## Known Threats and Weakness to IT and OT Environments

Known threats to both IT and OT environments uniquely impact utilities in the energy, transport, and water sectors. The most obvious threat to air-gapped OT environments is a malicious file on removable media, but other attack vectors include spear-phishing, software supply chain attacks, and more exotic attacks like using radio frequency, light, and acoustics.

Stuxnet, discovered in 2010, changed the perceived security of air-gapped systems by demonstrating how malware on removable media could be used to leap across isolated industrial control systems at a nuclear facility. Within Europe, multiple cyberattacks on Ukraine's energy sector, starting with phishing emails, have resulted in unscheduled widespread power outages since 2015.

Well before the 2020 attack on SolarWinds put software supply chain security into the spotlight, cyber attackers were targeting suppliers of utilities.

The US government in 2018 accused state-sponsored hackers of breaching air-gapped systems by spear-phishing users on the networks of key vendors that had trusted relationships with US power companies.[3] This gave the attackers access to the energy sector targets' air-gapped networks. The Cybersecurity and Infrastructure Security Agency (CISA) published an analysis of the attack.[4]

> **52% of Europe's energy sector OESs** did monitor IT and OT environments in a single SOC, while **16%** had a dedicated SOC for OT environments.[2]

Despite these known risks, the European cybersecurity agency ENISA's 2022 survey of NIS investments found almost a third (32%) of Europe's energy sector OESs did not monitor any OT service through a security operations center (SOC).[5] On a positive note, 52% did monitor IT and OT environments in a single SOC, while 16% had a dedicated SOC for OT environments.

## What Risk Management Practices Do Utilities Need to Implement to Meet NIS2?

NIS2 introduces a comprehensive set of risk management practices that both essential and important entities need to implement, including:

- incident handling
- business continuity, such as backup management and disaster recovery, and crisis management
- supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- basic cyber hygiene practices and cybersecurity training
- 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

NIS2 also states that entities should have:

- policies on risk analysis and information system security
- policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- policies and procedures regarding the use of cryptography and, where appropriate, encryption
- human resources security, access control policies, and asset management

Rather than allowing member states to determine incident reporting obligations, supervision, and enforcement, NIS2 sets out "minimum rules" for sectors and their obligations. Utilities will likely be subject by Member States to additional security compliance requirements beyond NIS2, such as ISA/IEC 62443, the international standard for industrial control systems.

"Member States should, where useful, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities."[6]

Essential utilities will also need to provide an "early warning" to the national Cyber Security Incident Response Team (CSIRT) or a competent authority within 24 hours of discovering a significant incident. They should also disclose whether the incident is "suspected of being caused by unlawful or malicious acts, and whether it is likely to have a cross-border impact." It should also, on a "best efforts" basis, notify customers of the threat.

Within 72 hours, the entity must follow up with an initial assessment of the incident, including its severity and impact, and if available, the indicators of compromise. A final report is required not later than one month after the submission of the incident notification.

NIS2 also established ENISA-operated EU-CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices, and agencies.[7]

## Will NIS2 Apply to the UK?

The UK will not transpose the NIS2 directive into UK law, however it has proposed updates to the existing NIS 2018 legislation. It proposes a new proactive supervision tier for the most critical providers, alongside the existing reactive supervision tier for other entities. The government also gains new "delegated powers" which allow it to update the regulations framework.

The UK government will be allowed to bring certain entities under NIS regulations if the entity provides critical services to an entity already in scope. It also aims to strengthen existing incident reporting duties to include significant incidents even if they don't affect service availability. The UK government has not given a timeline for implementing its updated NIS but on November 30 said it intends to pursue it "as soon as Parliamentary time allows."[8]

## What Fines Can Entities Face for Non-Compliance?

The UK, via competent authorities or the Information Commissioner's Office, can currently impose fines of up to £17 million for non-compliance. In the EU, "essential" entities can be fined up to €10 million or 2% of their total revenue worldwide.[9]

In the UK, the government is exploring cost recovery powers for regulators to cover the cost of enforcement.

## Discover how Fortinet can help.

utilities@fortinet.com

### References

1. EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation
2. NIS Investments 2022
3 Russian Hackers Reach US Utility Control Rooms Homeland Security Officials Say
4. Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors
5. NIS Investments 2022
6. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC
7. Eu CyCLONe
8. Cyber laws updated to boost UK's resilience against online attacks
9. What is NIS?

FORTINET

www.fortinet.com

April 19, 2023 09:31 AM

2085832-0-0-EN