

NIS2 Directive: secure your connected production

09 April 2025, 11:59

Thierry Coutelier
Olivier Gramaccia

Are you ready to meet the NIS2 Directive’s new cyber security requirements?

Connected sensors, smart machinery, collaborative robots... The Internet of Things (IoT) is transforming industrial production. Processes are becoming more efficient, productivity is improving and competitiveness is increasing. But this technological revolution also exposes your company to new cyber risks. The NIS2 Directive helps you raise your cyber security level.

The European NIS2 Directive came into force in Belgium on 18 October 2024. It requires businesses operating in critical sectors, including the manufacturing industry, to increase their cyber resilience.

NIS2: a legal requirement with strategic implications

If your company uses connected equipment (IoT) in its production, storage or logistics, you are potentially affected by the NIS2 Directive. And not just in technical terms: the management may be

held liable in the event of non-compliance. You therefore need to know your company's classification level in order to understand your obligations.

Ignoring NIS2 presents three major risks:

- **Operational disruption:** a cyber attack could paralyse your production lines, leading to financial losses and delivery delays.
- **Leaks of sensitive data:** confidential information about your products, customers, processes or finances could be compromised.
- **Reputational damage:** a security breach could erode the trust of your customers and partners.

To determine your NIS2 level, visit the website of the Centre for Cybersecurity Belgium (CCB):

Determine your NIS2 level

CyberFundamentals: the CCB’s compliance method

To help companies prepare, the CCB has introduced a framework called CyberFundamentals, setting out concrete measures tailored to an organisation’s size and risk profile. The framework is divided into four assurance levels: Small, Basic, Important and Essential. Other certifications such as ISO 27001 can facilitate NIS2 compliance. The cyber security measures that are implemented must be proportionate to the risks faced by the company.

If your company has more than 50 FTEs or exceeds €10 million in revenue, you will be classified at the Important level of NIS2 at the minimum. And even if you are not, following the recommendations of the Basic level will enable you to secure your systems effectively and meet your customers’ expectations.

The Basic level: the fundamentals for protecting your connected devices

The Basic level does not explicitly mention IoT, but several measures are directly applicable to these devices. Here is a selection, organised into five categories:

Identify:

- **ID.AM-1:** This measure consists of drawing up an inventory of physical devices, including all objects connected to the organisation’s network (IoT).
- **ID.AM-2:** Along similar lines to ID.AM-1, this measure focuses on an inventory of software platforms and applications. Again, the specific software and applications used by IoT devices must be listed.
- **ID.AM-3:** This measure focuses on documenting organisational communication and data flows. In the context of IoT, map your flows: where does IoT data come from, where does it go and how does it circulate?
- **ID.RA-1:** Identifying threats and vulnerabilities related to your IoT devices. This will put you in a better position to assess the risk and take appropriate action.

Plan:

- **PR.AC-1:** Managing IoT device credentials properly: avoid default passwords, apply strong rules and do not share them.
- **PR.AC-3 (key measure):** Securing remote access to IoT devices with strong authentication (such as MFA). In addition, isolating devices from the main network if possible (see PR.AC-5).
- **PR.AC-4 (key measure):** Applying the principle of least privilege to IoT devices: only grant users or systems the access that is necessary.
- **PR.AC-5:** Segmenting the network in order to isolate connected objects and limit the risk of propagation in the event of an attack.
- **PR.DS-1:** Encrypting data stored on IoT devices, and if possible, data in transit (PR.DS-2).
- **PR.IP-4 (key measure):** Regular backup and testing of IoT device data and configurations.
- **PR.MA-1 (key measure):** Keeping devices up to date with the latest security patches and updates.
- **PR.PT-1 (key measure):** Carrying out and testing regular backups of IoT device data and configurations. In the event of an incident, this means that devices and data can be restored to a pre-incident state.
- **PR.PT-4:** Maintaining IoT devices to ensure their security. Installing security patches and updates for operating systems and software used by IoT devices.

Detect:

- **DE.CM-1:** Monitoring the network for suspicious activity of IoT devices, using tools to detect traffic anomalies.
- **DE.CM-4 (key measure):** Detecting malware to protect IoT devices. Using anti-malware solutions to block infections targeting these devices.

Respond:

- **RS.RP-1:** Having an IoT incident response plan in place, including detection, analysis, containment, removal and restoring of compromised IoT devices.

Restore:

- **RC.RP-1:** Developing a plan to restore IoT devices and associated services after a security incident. This plan must include procedures for data restoration, device reconfiguration and service resumption.

Bear in mind: this list is not exhaustive. Other measures may be relevant to IoT security, depending on the context and the organisation’s specific needs.

Basic level cyber security measures have a significant impact on the security of connected objects (IoT). Implementing these measures as an organisation strengthens your data production, reduces the risk of cyber attacks, and increases your cyber resilience in an environment where IoT is increasingly prevalent.

Consult the complete guide to the Basic level:

CyberFundamentals - Basic level (PDF)

Important level: for mid-sized and large companies

Mid-sized to large organisations must go further. The Important level consists of the following additional measures:

- Identification of dependencies and critical functions (ID.BE-4)
- Introduction of resilience requirements (ID.BE-5)
- Assessment of supply chain risks (ID.SC)
- Secure configuration of equipment (PR.IP-1)
- Restriction of removable media (PR.PT-2)
- The principle of least functionality (PR.PT-3)
- Physical monitoring of facilities (DE.CM-2)
- Vulnerability analysis (DE.CM-8)

Implementing these measures will make your SME legally compliant and protect its operations, data, and reputation. Securing your IoT devices and their management will boost your company's resilience against cyber threats and ensure a prosperous future.

Summary:

- NIS2 has been in force in Belgium since 18 October 2024.
- It applies to many industrial SMEs using IoT.
- The Basic level of the CCB is a sound basis for securing your equipment.
- Sirris will support you in achieving compliance.

Sirris supports you towards compliance

Implementing the NIS2 Directive requires a clear strategy and a good understanding of the industrial implications.

Sirris can help you to:

- Assess your IoT risks.
- Identify your NIS2 level.
- Implement best practices.
- Strengthen your team training.

Take action now!

Protect your connected devices. Secure your production. Prepare for the future.

Contact a Sirris expert:

Thierry COUTELIER

Consult the guide CyberFundamentals – Basic level (PDF)

Also take a look at:

- The official NIS2 page – CCB
- The free training sessions of CyberActive (a project jointly financed by FPS Economy and the European Union)

Article written in connection with the IoT Standards Contact Point, with the support of FPS Economy.

Authors



Thierry Coutelier



Olivier Gramaccia