



NIS2 directive: how can Belgian industry defend itself against cyber threats?

04 April 2025, 10:37

Thierry Coutelier

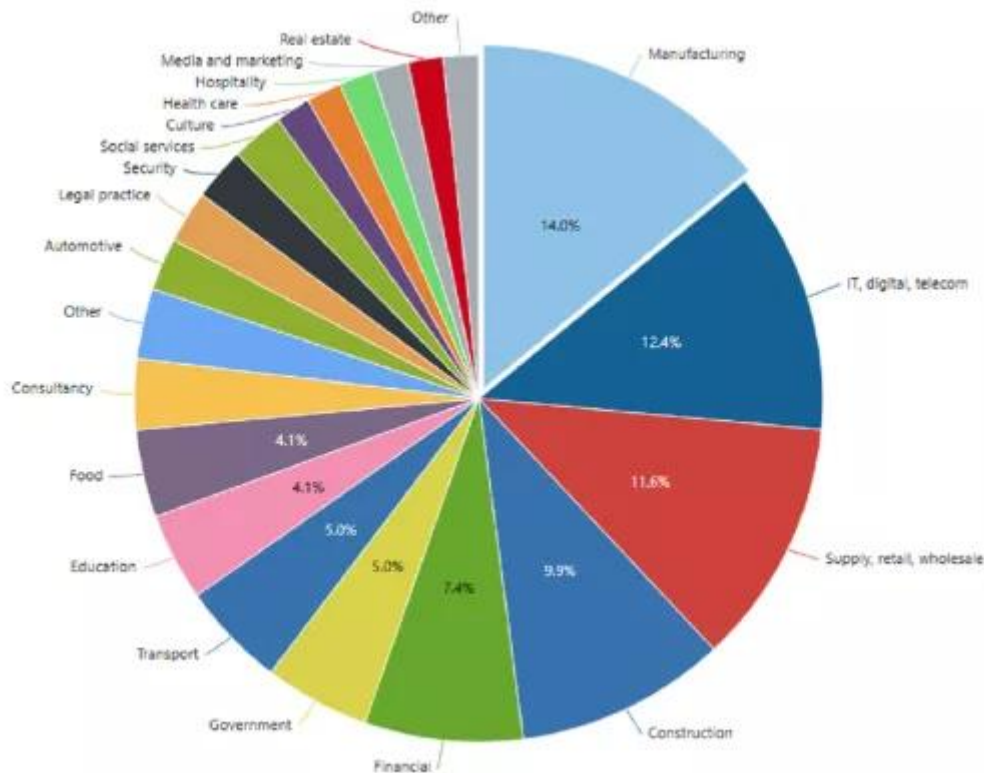
At a time when industry is accelerating its digital transformation, cyber-attacks are multiplying, seriously testing the resilience of manufacturing companies. With the recent entry into force in Belgium of the European Directive NIS2, companies must henceforth reinforce their cybersecurity or else face sanctions. From regulatory requirements, and common vulnerabilities to adopting good practices, here's how to anticipate and effectively protect your business.

The digital transformation offers new opportunities to industry: innovation, process optimisation, cost reduction and new sources of revenue. But this digital revolution has also been accompanied by a disquieting increase in cyber-attacks. Today, every organisation is a potential target, from big multinationals to local SMEs. Ransomware that paralyses production chains, massive theft of sensitive data, targeted attacks on strategic suppliers: the incidents are multiplying and becoming more sophisticated.

As of 18 October 2024, the entry into force in Belgium of the European Directive NIS2 (Network and Information Security) imposes strict rules on manufacturing businesses in order to prevent these risks and reinforce their cyber resilience.

A warning for Belgian manufacturers

Several recent studies have signalled the upsurge in cybersecurity incidents affecting the industrial sector. In 2023 and 2024, the Centre for Belgian Cybersecurity (CCB) identified, respectively, 120 and 100 attacks by cybercriminals against Belgian organisations. The manufacturing sector is a pillar of the Belgian economy, but it is often less well protected than other sectors.



The consequences of a cyber-attack on industrial systems can be dramatic: prolonged stoppage of production chains, considerable financial losses, rapid worsening of reputation among clients and partners. In certain extreme cases, even the security of employees is compromised when cybercriminals take over critical systems. Not to mention the loss of sensitive data, such as industrial secrets or strategic information.

NIS2: new reinforced requirements

Faced with these growing threats, the European Union has hardened its tone with NIS2, the new directive on the security of networks and information. The aim of the directive is to strengthen the resilience of sectors regarded as important or essential, among them the manufacturing industry. In practice, NIS2 henceforth imposes obligatory measures on Belgian businesses. These include:

- regular assessment of cyber risks in order to identify vulnerabilities;
- development of incident response plans in order to react quickly to an attack;
- reinforced checks on suppliers and subcontractors;
- financial sanctions in the event of non-compliance.

At Sirris, we have found that numerous companies still underestimate the impact of non-compliance with NIS2. Yet, the sanctions can be severe, both in financial and reputational terms. More than just an obligation, cybersecurity is now a crucial area of focus for competitiveness and industrial resilience.

5 common vulnerabilities in industrial cybersecurity

Industrial companies, whose IT (information technology) and OT (operational technology) are now closely interconnected, are especially vulnerable. Among the most common vulnerabilities observed in this industry are:

1. **Absence of network segmentation**

When IT/OT systems are interconnected without a clear separation, one single breach is all it takes to compromise the entire infrastructure.

2. **Outdated software**

A number of factories are still using operating systems and software that are several decades old, and have not been updated. These are an easy target for hackers.

3. **Phishing and social engineering**

Cybercriminals exploit human weaknesses: a simple fraudulent e-mail is all it takes to infiltrate a system.

4. **Poor access management**

Access to sensitive systems is open to too many employees, which allows cybercriminals to exploit secure accounts and gain access.

5. **Breaches in the supply chain**

Suppliers and service providers can be entry points for cyber-attacks that affect the entire industrial infrastructure.

These vulnerabilities, well known among cybercriminals, require constant vigilance and reinforced protective measures.

Five key measures to reinforce your security

No business is entirely invincible, but there are simple and effective steps that you can take to significantly reduce the risks:

1. **Segment IT and OT networks**

Separate the IT and OT environments in order to limit the scope of an attack and to prevent a problem in a bureaucratic system from paralyzing production.

2. **Keep software up to date**

Updating security is essential for rectifying vulnerabilities exploited by hackers. An obsolete system is an easy target.

3. **Train and inform employees about cyber risks**

The employees are the first line of defence. Raise awareness about phishing attacks, secure passwords and good practices in cybersecurity.

4. **Reinforce access management**

Access to critical systems should be limited to authorised personnel only. Multi-factor authentication (MFA) and the management of access rights by role are effective solutions.

5. **Secure the supply chain**

Suppliers must respect strict cybersecurity standards. Check that they have adequate checks in place to avoid exposure to indirect vulnerabilities.

These good practices are accessible to all companies and help prevent considerable financial losses. At Sirris, we believe that small actions today can prevent major catastrophes tomorrow.

Anticipation means greater resistance

Cyber threats are evolving rapidly, and industry can no longer ignore the challenges connected with cybersecurity. Compliance with NIS2 may be a challenge, but most of all it represents an opportunity for industrial enterprises to reinforce competitiveness and resilience. Investing today in cybersecurity guarantees operational continuity and protects the future of industry.

Whether you are in manufacturing or digital services, CyberActive, an initiative in which Sirris is a partner, will help you to navigate the world of cyber threats by means of training courses, pedagogical support and explanatory videos on all aspects of cybersecurity.

[Explore the full agenda and secure your spot](#)

CyberActive is an initiative of Sirris, Howest, Catholic University of Leuven and Brussels University (VIB/ULB).
Financed by the Ministry of Economy and the European Union (Next Generation)

Authors



Thierry Coutelier