NIS directive and supply chain security: how does it concern you?

09 September 2022, 15:01

Tatiana Galibus

Have you already heard of the NIS Directive? The majority of manufacturing companies are not yet aware of the importance of this regulation across the EU. At Sirris, we follow-up the implementation of this directive in Belgium, because the rules established by it touch you directly if you work in one of Belgium's 3,000 manufacturing SMEs, and even if you work for a provider, machine builder, digital service supplier company.

What is it ?

(ec.europa.eu)

The NIS(-1) Directive was accepted by the EU in 2016. It was the first cybersecurity legislation on European level. In Belgium, it was applied as NIS Act in 2019. What are the obligations under the current NIS?

Member States	• develop National Cybersecurity Strategies • collaborate cross-border • identify **Operators of Essential Services (OES)** in: energy, transport, banking, financial market infrastructures, healthcare, drinking water, and digital infrastructure.
OES operators	• take minimum security measures • report significant incidents.
Providers of key digital services	• comply with these security and notification requirements

NIS-2 was proposed by the EU in December 2020 due to the increase in cyberattacks and their devastating impact. Among others, it includes the following enhancements:

- more sectors and entities in the scope of cybersecurity
- extended security requirements
- personal involvement and responsibility of managers and boards
- strict penalties and higher amounts
- detailed incident reporting obligations
- focus on strengthening supply chain security

You probably haven't heard much of it yet, because these rules are not yet widely adopted. However, it is expected that by 2025 the situation will change with Belgian NIS-Act acceptance.

Why is it important?

In short, the EU proposes to tighten the requirements for suppliers, increase penalties and impose personal responsibility on CEOs and board. Strengthened and personalized regulations will touch all companies involved with your supply chain interactions and will inevitably change the way you collaborate with the suppliers and provide products to customers. Being secure will become much more essential for business continuity.

For some, it may sound scary, for others, already preparing for the future, it is no surprise. Cybersecurity takes its place as added value to your product and sooner or later you will not be able to sell without this `feature`.

And what if you choose to ignore these changes in legislation? What does it mean for an SME? It definitely means losing customers if you are not secure enough. The majority of companies are involved with more and more complex and elaborate supply chain interactions which are often not yet secure. For example, answering 'yes' to any of the following questions means you are *not secure in NIS terms*:

- Do you give admin rights to external collaborators without specifying the machines and access control policy?
- Do you avoid regular monitoring of external connections?
- Do you forget to review the ports and tools used for remote maintenance?

Am I secure?

Unfortunately, there is no uniform questionnaire related to your supply chain chain security and NIS-2 directive. We are working on such automatic tool at Sirris within the scope of Cornet project Cybersecurity 4.0**.**

Currently, Sirris proposes free 1 hour cybersecurity intakes for manufacturing companies with a focus on a supply chain, during which we will ask you some questions and propose solutions to the critical vulnerabilities if discovered. Interested in such an intake? Contact us!

What to do next?

Be prepared. Be ahead of hackers. The cybersecurity landscape is changing every day and keeping your finger on the pulse is essential: with attacks getting more and more organized, security should be more collaborative and agile, which means ensuring the security of the whole supply chain.

Sirris runs a 2-month education trajectory with a hands-on practical focus to help manufacturing companies with cybersecurity. We offer individual coaching sessions and masterclasses on your premises, in order to help you design your own cybersecurity strategy and eliminate specific risks.

Check our collective and individual offerings here!

Further reading:

ENISA: https://digital-strategy.ec.europa.eu/en/policies/nis-directive

CCA Belgium: https://www.cybersecuritycoalition.be/nis-2-where-are-you/

Authors

Tatiana Galibus