Alarming reality of cyberattacks in manufacturing SMEs

17 August 2021, 02:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

In times of digital transformation and Industry 4.0 cybercrime has never been more real for Belgian SMEs. Any company without sufficient security resilience can become a victim. To be able to shield themselves from such attacks, SMEs need a tailor-made strategy and a clear roadmap for resilience, but there are still barriers to overcome. Sirris can help!

Cyberattacks are no longer a matter of a big company, but a common issue for SMEs. Each year, threats to connected manufacturing reach their critical point. Currently, there are more than 30.000 cyberattacks registered with a 20% annual increase in incidents. Cybercrime has never been more real for Belgian SMEs. Digital transformation and Industry 4.0 pose a serious risk to enterprises as legacy machines with high security risk are being connected, and data is being collected and exchanged between sites without any control. Any company without sufficient security resilience can become the victim of cybercrime and the consequences of security breaches - interrupted operations, data loss and a spoiled reputation - can take down business or take months or years to recover from. Therefore, to be able to shield themselves from such attacks, SMEs need a tailor-made strategy and a clear roadmap for resilience.

Currently, we identify two mayor barriers for SMEs preventing them from realising or implementing their cybersecurity strategy:

- the cyber services offered by commercial-oriented professional companies in Belgium are too expensive and unreachable for most of SMEs that have limited resources.
- the existing cybersecurity standards and guidelines are either too general or technical, which makes it hard for people in manufacturing SMEs with limited knowledge and background to understand and make use of them to realise their cybersecurity strategy.

New agile approach

Understanding these pain points, Sirris developed a new agile approach to cybersecurity aiming to help SMEs to realise their cybersecurity strategy without investing too much effort and financial resources.

Understanding that trust is key in order to get the level of information we need, we start with a free 1-hour online intake session. The goal of this low entry approach is to get companies starting as soon as possible to increase their cybersecurity level. Also, in this session they can verify whether the Sirris approach to cybersecurity is what they need for their company.

In this first session we focus briefly on three domains:

- IT (office) infrastructure
- OT (production) infrastructure but also on the integration between IT and OT
- data security aspects (eg. is the intellectual property enough protected etc.)

Visuals, data and OT (three domains)

After this session we provide a structured report with the issues we already could detect and add some advice on how to deal with them. Each topic also receives a maturity level estimation, so companies know where they stand and to what level they should evolve.

Based on the recommendation of this document a company can start right away improving their overall cybersecurity.

Cybersecurity scan

If the company wants to go further and obtain a more in-depth cybersecurity scan we go on site and go much deeper in all the different topics based on the result of using security scan tools and interviews.

As a result of the scan we provide a structured table of assets, vulnerabilities and risks, which makes it easy for a company to make a decision on the next steps and priorities towards resilient cybersecurity.

Domain	Asset	Controls in place	Vulnerability	Risks

OT security	IoT sensor devices	Connected through firewall Restricted ports Restricted access time	• Firmware vulnerability • Insufficient audit • Inadequate authentication	Critical: • Mistake in the firmware code can cause buffer overflow • Adversary can easily brute force into the device by guessing the weak password . Middle: • Unnecessarily open port allows to realise Ddos attack on a device Low: • Incorrectly configured monitoring results in the excess of false positives
Data security	Personal employee data	Stored on a protected server Restricted access	• Weak cryptography • Insufficient access control • Absence of data classification	Critical: • Adversary gets access to private data and publishes it • Adversary misuses the PII data to breach into employee account • Adversary uses PII data to impersonate company managers for spear phishing Middle: • Adversary encrypts or deletes the PPI data

This structured table allows to refer to possible problems and outline them directly, in order to react faster and more efficiently in place accordingly.

Time for action

Would you like to know more about our approach or participate in a free 1-hour intake? Contact security@sirris.be or Tatiana.Galibus@sirris.be to register.

Want more information about cybersecurity in manufacturing? Do you have a specific question? ***Get in touch or consult our web page****!*

(Source banner: iStock)

Authors

Annanda Rath

Christophe Michiels

Tatiana Galibus