Future-proof cybersecurity, also for SMEs!

14 September 2021, 02:00

Annanda Rath
Tatiana Galibus

In times of digital transformation and Industry 4.0, cybercrime has never been more real for Belgian SMEs. Companies with insufficient security resilience are potential victims. SMEs need a tailored strategy and a clear roadmap for protection now and in the future. Sirris and Agoria meet you halfway with a new approach, tailored to SMEs!

Cybercrime has never been more real for Belgian SMEs, now that large companies are no longer the only targets of cybercriminals. More than 30,000 cyberattacks have currently been recorded with a 20 per cent annual increase in the number of incidents. The digital transformation and Industry 4.0 pose a great risk to enterprises, as outdated machines are associated with a high security risk and data is collected and exchanged between websites without any control. Any business that does not have sufficient security resilience can become a victim of cybercrime, and the consequences of security breaches - business interruption, data loss and reputation damage - can undermine a company, often with major short- and long-term consequences.

In order to protect themselves against such attacks, SMEs from different sectors need their own approach, and this is what Sirris and Agoria have worked out in a broad offering of very targeted and practical workshops, adapted to the target group, sector and type of company.

From intake to cybersecurity scan

Sirris has developed a new flexible approach to cybersecurity to help SMEs realise their cybersecurity strategy without investing too much effort and financial resources. We start with a **free online intake session of 1 hour**. After this session, we provide a structured report with the problems already detected and give our advice on how to tackle these problems. The company can immediately start improving its overall cybersecurity based on the recommendation(s) in this document.

If the company wants to go a step further and wants a more **in-depth cybersecurity scan**, we visit the premises and discuss all the individual points based on the results of security scans and interviews in more detail. The result of the scan provides a structured table of assets, vulnerabilities and risks. This makes it easier for the company to decide on next steps and priorities for a more resilient cybersecurity.

Read more about this approach here.

Workshops for any type of company from any sector

Looking for concrete tips & tricks for cybersecurity?

We'll help you prevent a digital lockdown of your company (or worse) during the no-nonsense, highly practical 'Cyber secure in 30 steps' masterclass. We will discuss a risk-based approach that should form a fundamental basis for every company, focusing on the cyber security of its internal resources. We will explain to you 30 achievable and immediately applicable steps to take your company's cybersecurity to a significantly higher level. If you apply these 30 steps correctly, you will already have found a very nice balance between the risk you run and the investment you make in cybersecurity.

As a manufacturing company, finding your way in cybersecurity?

Cybersecurity is a hot topic for many manufacturing companies. Gaps in cybersecurity can lead to data loss, financial losses and reputational damage. The webinar 'Cybersecurity for manufacturing companies' presents he most important cybersecurity solutions and explains best practices to improve cybersecurity in manufacturing, from both an IT and OT (Information Technology and Connected Shop Floor) perspective. This webinar focuses on pragmatic solutions that are also feasible for SMEs.

The 'Cybersecurity for manufacturing companies' masterclass teaches you how to take safe steps towards Industry 4.0 via a feasible step-by-step roadmap towards resilient cybersecurity. We provide you with the knowledge in a pragmatic hands-on format to give you an in-depth understanding of all safety aspects of your transition to Industry 4.0.

Based on the results of the study 'Cybersecurity in the Belgian Manufacturing Industry', Sirris and Agoria decided to bring manufacturing companies together in a learning network around the theme of cyber security in OT, more specifically the ability to detect threats and anomalies in the production environment. After all, significantly improving detection capabilities is, in many cases, one of the least invasive ways to significantly increase the cyber resilience of the production environment.

How to survive security assessments as a digital start-up or scale-up?

Have you, as a start-up or scale-up, after months of demos and so on, come up against negative advice from TPSA-assessors within a large company? Risk management and the ‘trust decision’ all too often come at the end of the buyer journey and insufficient trust is the main reason why things still ultimately go wrong. There is still a lot to learn about this 'TPSA' domain, from each other and from the perspective of the assessor. That is why we are bringing together a group of digital product and service companies in a learning network around the theme of surviving a security assessment.

(Source banner: iStock)

Authors

Annanda Rath

Tatiana Galibus