RSECURE

# Cyber support for small businesses

Protect your business with our customized services !

MADE IN LUXEMBOURG

## IS CYBERSECURITY REALLY USEFUL FOR SMALL BUSINESSES?

Cybersecurity is no longer limited to large companies or public institutions.  Very small businesses (VSBs), often perceived as less exposed targets, are increasingly finding themselves in the crosshairs of cybercriminals.

With limited resources, sometimes rudimentary protection, and uneven awareness, VSBs represent an easy entry point for cyberattacks. Yet a single security breach can have devastating consequences: loss of customer data, service interruption, damage to reputation, or even the closure of the business.

So, in the face of these very real threats, is cybersecurity a luxury or a necessity for VSEs?

### CYBER STATISTICS IN LUXEMBOURG

- 1,466 attacks per week
- +82% increase in the number of attacks since the last four months
- 62% of breaches are related to information leaks
- 18,645 €: Average cost of a cyberattack for a company
- 1 in 8 companies report that attacks have cost them more than 230,000€

## INCLUDED SERVICES

- Awarness
- Phishing campaign
- Monitoring
- Cybersecurity monitoring
- Audit support

**EMPLOYEE AWARENESS:** Training and raising awareness among your employees about the various risks associated with cybersecurity plays a key role in protecting your IT systems. Training teaches employees how to recognize the most common threats and develops their vigilance.

**PHISHING CAMPAIGN :** Once employees have been trained, it is essential to test their reflexes regularly using tailored and personalized phishing campaigns. Do they know how to detect warning signs such as suspicious sender addresses, spelling mistakes, "urgent" attachments, etc.?

**MONITORING :** is a process of continuous and proactive monitoring of a company's IT security devices, including antivirus software, firewalls, cloud solutions such as Microsoft 365, intrusion detection systems, and other protection tools. It is not simply a matter of checking that they are working properly, but of analyzing activity logs, alerts, and network behavior to anticipate threats and respond quickly to incidents.

**CYBERSECURITY MONITORING :** consists of continuously monitoring developments in the cyber threat landscape, including new attack techniques, emerging vulnerabilities, software vulnerabilities, and cybersecurity trends. During our meetings, we share the most relevant and recent information with you, along with targeted and pragmatic recommendations to strengthen your security posture.

**AUDIT SUPPORT :** Because the cyber world is constantly evolving, and national and European regulations are becoming increasingly numerous and specific, our experts are here to assist you with compliance audits and any questions you may have about cybersecurity.

## OPTIONS

- Online training platform with phishing alert button
- "SOC tranquility": Security Operation Center available 24/7 (service that tracks and blocks attacks on devices connected to the company network)
- Implementation of security policies tailored to small businesses: IT charter, incident management, etc.