ARTICLE: “Why Cybersecurity Training Is Necessary for SMEs and Public Administration”

Today, cybercrime has become an increasingly common form of attack. CrowdStrike warns that between 2023 and 2024, cyberattacks rose by 75%. This may be due to how easy they are to be structured (attackers can operate from home without having to travel and with only minimal IT knowledge) or how fast they can be executed (often with just a simple click).

Cyberattackers pursue many targets, but the main one is usually financial gain, achieved by damaging the data that companies manage. In addition, most cyberattacks stem from human error: incorrect configurations, opening malicious emails, using weak passwords, among others. Recent studies reveal that human error is responsible for up to 95% of security breaches in companies.

One type of attack that is growing significantly is supply chain–focused attacks, which exploit vulnerabilities in suppliers or partners to gain access to systems. For this reason, managing cybersecurity within the supply chain will be an unavoidable challenge.

Given all this, one could conclude that strong protection and proper cybersecurity training could prevent or limit the damage from these attacks. However, there are still companies (both small/medium-sized enterprises, and public institutions) that lag behind, lacking the security measures needed to confront these daily threats, which are increasingly difficult to detect (largely due to attackers’ use of AI).

Small businesses often think, “We’re small; no one will attack us,” or “We’re not as interesting as large corporations,” but this is completely false. We must keep in mind that:

- Attackers often prefer small businesses because they tend to have weaker protection and lower response capacity, making them attractive targets.
- The belief that “we’re not interesting…” is entirely wrong, as SMEs hold data that is highly valuable to attackers, such as customer information (ID numbers, bank accounts, addresses…), invoices, and access to online banking.
- The impact on an SME is twice as severe as on a large company due to their limited resources. In some cases, a single cyberattack has forced a small business to close its doors due to the devastating consequences. Conversely, large companies are better equipped to handle such incidents. Cybersecurity Magazine notes that 83% of small and medium-sized businesses are not prepared to recover from the financial damage of a cyberattack.

Therefore, cybersecurity training is both essential and highly important. It brings benefits such as:

- Reducing cyberattacks caused by human error (employees).
- Strengthening security measures against attacks.
- Being able to anticipate and detect threats more easily.
- Improving response capabilities during cyberattacks.
- Encouraging good cybersecurity practices both inside and outside the organization.
- Protecting personal data as well as that of customers and suppliers.
- Reinforcing public trust.

Train in cybersecurity – Protect your business