ELEARNINGNEWS ARTICLE

Year 9 - number 327 Wednesday 26 march 2025

Growing Cyber Attacks: The Agreement Focused on Prevention

The State Police and Confindustria join forces to strengthen the cybersecurity of companies. But without training, no defense is truly effective.

No company is safe. In recent years, cyber attacks have become increasingly sophisticated and frequent, indiscriminately targeting businesses of any sector and size. The data is clear: between 2021 and 2022, reports of cyber crimes filed by companies more than doubled, going from 5,000 to over 13,000, then stabilizing around 12,000 in 2023.

The techniques used by cybercriminals are increasingly advanced and targeted. **Ransomware**, for example, locks company systems and demands a ransom to restore data. Other attacks aim to steal sensitive information, which can be used for fraud or sold on the dark web. The problem doesn't only concern large companies, which invest in advanced security solutions, but especially affects small and medium enterprises, often less equipped to counter the threat.

The Agreement between Police and Confindustria

To respond to this emergency, **the State Police and Confindustria Brescia have signed a memorandum of understanding** with the aim of strengthening the cybersecurity of companies. The agreement is based on three main actions.

1. **Increase the cyber resilience of companies**: through the sharing of compromise indicators, businesses will receive timely alerts about ongoing threats, allowing them to strengthen their defenses before it's too late.
2. **Define effective procedures in case of attack**: a security system is not only effective in prevention, but also in the ability to respond quickly to incidents. Companies will be guided on how to react effectively to limit the damage of an attack.
3. **Enhance training on cybersecurity**: the most crucial point. As highlighted by the director of the Cyber Security Operations Center of Lombardy, Manuela De Giorgi, most cyber attacks rely on the unwitting collaboration of the victim. A simple click on a fraudulent link can open the door to devastating intrusions. No security software can be effective if its users are not aware of the risks and cannot recognize threats.

The Human Factor: The Weak Link in Cybersecurity

Hackers no longer limit themselves to looking for flaws in computer systems: they target people directly. Techniques of **social engineering** such as phishing and spear phishing aim to deceive employees to obtain access credentials or install malware. Often, a seemingly innocent email or a well-studied phone call is enough to compromise entire corporate infrastructures.

Yet, many companies continue to underestimate this aspect, focusing only on investments in protection software and advanced firewalls. But no technological barrier can replace a widespread culture of cybersecurity in the company. If employees are not adequately trained, they risk being the entry point for an attack, nullifying any cyber defense strategy.

This vulnerability is even more evident in small and medium enterprises, where cybersecurity is often perceived as an accessory cost and not as a necessity. Many SMEs do not have a dedicated IT team and delegate security management to non-specialized figures, increasing the risk of suffering devastating attacks. Precisely for this reason, the protocol signed between the State Police and Confindustria has a strategic value: to promote awareness and provide concrete tools to protect the Italian business fabric.

Cybersecurity and Training

If the human factor is the most vulnerable point in cybersecurity, then training becomes the first line of defense. However, teaching companies and their employees how to recognize and counter cyber threats is not simple: effective tools, constant updates, and methodologies that promote continuous learning are needed.

In this context, **eLearning proves to be the ideal solution**. Online courses allow companies to train their staff flexibly, with modules always updated on new threats and attack methods.

One of the most common mistakes in companies is considering cybersecurity as an exclusively technological problem, delegating it to IT departments without actively involving all employees. In reality, cybersecurity is a shared responsibility.

- **Executives and managers**: they must know prevention strategies and risk management to make quick decisions in case of attack.
- **Operational employees**: they are the primary target of hackers and must be able to identify phishing attempts and social engineering.
- **IT and security teams**: they need constant updates on new threats, vulnerabilities, and defense strategies.

A wrong click by an employee can compromise the entire company system. Precisely for this reason, training must be widespread at all levels, creating a culture of cybersecurity within the company.

Mega Italia Media offers an eLearning course designed to train employees and managers on cyber threats, providing concrete tools to prevent attacks and protect company data.

The course include:

- Techniques for identifying and preventing cyber attacks such as phishing, malware, and ransomware.
- Cyber defense strategies to protect networks, data, and company systems.
- Regulatory insights on cybersecurity.

Investing in training is the most effective solution to reduce risks and ensure operational continuity. **Discover the course**.