ELEARNINGNEWS ARTICLE

Year 8 - number 275 Wednesday 07 february 2024

The costs of failing cybersecurity for companies

Let's find out what the impacts and costs of a lack of corporate cyber security are and how to mitigate cyber risks in companies.

Last December, a **serious cyber attack hit the Italian Public Administration**, paralyzing numerous digital services and causing problems with electronic invoicing.

The attack was started by targeting Westpole, a company that provides cloud services to PA Digitale, a company that in turn offers software and programs for municipalities and other public bodies. Once its security was breached, the hackers took out the Urbi software, used to manage registry and citizen services, blocking the systems of around 300 public bodies at a local and national level.

This latest attack on the IT infrastructure of the Public Administration highlights the importance of guaranteeing maximum **security in data processing** in all companies.

In this article, we will analyze the impact of cyber attacks on companies, focusing in particular on the costs of missing cyber security and on ways to mitigate cyber risks.

The impact of a cyber attack on companies

Depending on the type and quantity of data processed, the impact of a cyber attack can vary significantly. Generally speaking, the loss or theft of data exposes the company to legal, economic and reputational damage.

First of all, the damage generated by a cyber attack requires the **intervention of qualified personnel** in the cyber security sector. The blocking of systems could also lead to the **temporary interruption of company production** or the provision of a service, with consequent **losses of profit**.

News of a compromise of its IT systems also affects the **company's reputation**, generating a negative impact on customers and partners.

With reference to direct costs, however, failure to comply with the security measures of the GDPR entails **heavy penalties**, as well as compensation for the owners of sensitive data. And, in some cases (for example in the case of ransomware attacks) it may be necessary to **pay a ransom** to regain possession of the data and functionality of your systems.

Finally, cyberattacks can have **consequences for the health and well-being of workers**, who may feel a burden of guilt, confusion or frustration. For further information on this topic, also read " **Cyber ??attacks: what impacts on the health and safety of workers?**".

How much does a data breach cost businesses?

According to IBM's **Cost of a Data Breach Report 2023**, the global average cost of a data breach reached **$4.45 million in 2023**, an increase of 15% over the past 3 years.

Also at a global level, the report found that 95% of companies interviewed have suffered more than one breach and are inclined to **blame the costs of the attacks suffered on customers** (57%) rather than **increase investments in security** (51%).

As regards the **Italian panorama**, the overall average cost of data breaches is equal to 3.55 million euros. On average, it takes **235 days to identify and contain a cyber threat**, of which 174 to identify a breach and 61 to contain it.

The main attack vectors are social engineering, phishing, and stolen or compromised credentials. The most expensive ones are: malicious insiders and compromise of company emails.

How to mitigate IT risks in the company?

- Carry out a careful **risk assessment** that highlights any weak points.
- Implement cybersecurity policies and procedures.
- Use security technologies such as firewalls, data encryption, access controls, antivirus, etc.
- Adopt backup and recovery systems to guarantee the availability and integrity of data, as well as their recovery.
- Raise staff awareness of the importance of cyber security and provide adequate training on IT security.
- Implement real-time cyber threat detection and monitoring systems.
- Manage cybersecurity incidents in a timely manner.

The importance of the human factor in mitigating cyber risks

When talking about cybersecurity, it is very important to be aware that technologies alone are not enough. For them to be effective, it is necessary to develop digital security strategies that take into consideration primarily the human factor and therefore the preparation and protection of personnel materially involved in the use of IT systems and data processing.

Human error (opening phishing emails or mismanaging passwords) is in fact considered the root cause of 90% of cybersecurity breaches and can expose organizations to serious consequences, such as the installation of malicious software on the network corporate.

Read also: **How and why train employees on cyber security?**

For further information on cyber security in the company, read also:

- **Cyber ??Risk: the defense of companies**
- **Corporate cybersecurity: data on attacks**