ELEARNINGNEWS ARTICLE

Year 5 - number 170 Wednesday 1 september 2021

Cyber risk: the defense of enterprises

New challenges for enterprise cybersecurity have been brought by remote working and the growth of digitization

Our computing devices (private and corporate) contain a huge amount of data, very interesting for **cyber criminals**.

We have seen that defending against cyber attacks is possible and depends mainly on **training**, also in **eLearning**.

Over the last few years, **remote work** and communications via **video conferencing** have brought to light new critical issues for companies to effectively defend their cyber security.

Cyber attacks don't just affect large enterprises - quite the opposite. About 50 percent of cyber attacks are directed at SMBs, with an average cost per attack of nearly 200,000.

What are the 8 most common attacks on the enterprise cybersecurity system?

1. Advanced Persistent Threat (APT)

APT is a threat carried out invisibly and for very long periods of time on a network or a computer, with the aim of stealing confidential information or making some services of the attacked entity unusable. Very often this is cyber espionage and is implemented by state entities. In fact, hackers using ATP often act for political-economic motivations.
If the same level of attention from cybercriminals were directed against a business it could prove devastating.

2. Phishing

This is the most common computer scam, carried out by sending an email with a counterfeit logo and email address (for example, of a credit institution or an e-commerce company), in which the recipient is asked to perform a certain action, for example provide confidential data (credit card number, password for access to home banking, etc.) or click on a link that actually leads to a malicious site; motivating this request with technical reasons. Once the action is complete, the hacker can access computer systems and collect personal or business information.

3. Denial of Service (DoS)

DoS indicates a website malfunction due to a cyber attack in which the resources of the computer system itself are deliberately depleted through two methods:

- Custom-created data: this method involves sending specific data to a system that is capable of causing an error within it, preventing it from functioning.
- Flooding: this method involves overloading a system to slow it down so that it is no longer able to function.

The result is inevitably website downtime and consequent loss of profits.

4. Internal attacks

Internal attacks, which are becoming increasingly worrying, involve a user who has the credentials to access the company's IT system (employees, external collaborators).

5. Malware

The term malware defines any computer program downloaded onto a PC without the user's knowledge and used to cause serious damage or data breaches. Malware is often used on corporate and private devices, but it is also commonly used as a form of international government espionage.

6. Password Attacks

Password attacks, also known as brute force attacks, are attacks in which a hacker enters different password combinations in an attempt to gain access to a network. This is often done with the help of automated systems.

7. Ransomware

Ransomware is a type of malware that restricts access to the device it infects, requiring a ransom (ransom) to be paid to remove the restriction. Unfortunately, payment does not always result in the return of the account.

8. Man-In-The-Middle (MITM)

A man-in-the-middle attack occurs when a third party intercepts a communication between two parties. This third party gains access to the communication by listening in or monitoring activity, gaining access to any information shared, including login credentials, personal information or more.

Risk management: new challenges

According to the VIII Observatory on the diffusion of **risk management in medium-sized companies** carried out by Cineas in collaboration with Mediobanca, the health emergency that has struck Italy and the rest of the world in recent months was not on the horizon of mapped and potential risks, but it will not prevent more than half of the companies questioned (54.7%) from maintaining their planned investments. As mentioned, however, remote working and the advancement of corporate digitization have opened up new challenges on the security front for all companies that require the development of dedicated strategies and plans in terms of cybersecurity and protection of sensitive data. The survey, which involved a sample of 339 companies, shows how, today, companies see threats mainly in two areas: firstly, accidents at work, but also the cyber risk corollary of the increasing dependence on technology.

Moreover, "in relation to the development of remote work, there is a risk of loss of applied skills. We need to improve smart management, the management of people remotely, in order to ensure the cohesion of the teams, to emotionally support the collaborators, to train them more intensely, to clarify even more clearly the expected objectives and the stages to achieve them," declares Massimo Michaud, President of Cineas.

Translated with www.DeepL.com/Translator