ELEARNINGNEWS ARTICLE

Year 5 - number 171 Wednesday 8 september 2021

Corporate cybersecurity: the data on attacks

One in every 10 incidents analyzed has a high severity level

According to anonymized metadata voluntarily provided by Kaspersky MDR customers, a cybersecurity and digital privacy company that has been operating globally for more than 20 years, one in 10 (9%) of the cybersecurity incidents blocked could cause severe disruption or unauthorized access to customer resources. The majority of incidents (72%) were of medium severity.

We have already seen what are the main **types of cyber attacks** that can affect the performance of enterprise resources or lead to instances of data misuse.

"Research has shown that targeted attacks are common: more than a quarter (27%) of organizations have experienced one. Nearly all industries, with the exception of media and transportation, experienced high severity incidents during the period analyzed. Most often, critical incidents affected organizations in the public sector (41%), followed by IT (15%) and financial (13%). Nearly a third (30%) of incidents were related to targeted man-made attacks while 23% of high severity incidents were classified as high impact malware (including ransomware). In 9% of cases, cybercriminals gained access to corporate IT infrastructure using social engineering techniques. Current APTs have been detected along with artifacts from previous advanced attacks. This suggests that if an organization responds to a sophisticated threat, it is often attacked a second time, often by the same cybercriminal. Additionally, in organizations victimized by APT, experts have observed signs of simulating an adversary's behavior, such as red teaming, or an assessment of a company's operational security capabilities through a sophisticated attack simulation."

The good news is by being aware of the risks you can have effective means to address them, for example by taking advantage of dedicated threat detection and blocking services, upgrading the professional training of the IT team, and very important, but often underestimated step, **basic cybersecurity training** of all staff. In fact, increasingly, cyber attacks begin with phishing or other social engineering techniques.

Translated with www.DeepL.com/Translator