ELEARNINGNEWS ARTICLE

Year 4 - number 127 Wednesday 23 september 2020

Defending privacy in eLearning with Artificial Intelligence

Is it possible to protect computer systems with artificial intelligence?

In the course of 2020 we were able to see for ourselves how **cybersecurity** is a fundamental aspect of a digital world.

Globally, news of **cyber attacks** on databases of schools, universities, distance learning and collaboration platforms abound. The risk is serious, if you think of the value that that information has for cybercriminals, and must be managed and calculated. To better understand the situation we have deepened the experience of a U.S. company operating in the field of cyber defense based on artificial intelligence. What does this mean? In this case, the response technology to cyber attacks is autonomous and self-learning.

"It was discovered that, in April, a **university in the United Kingdom** was hit by a ransomware attack, a type of malware that blocks access to the computer system in seconds by demanding a financial ransom in exchange for restoring functionality. Hackers tried to access both staff and students' computers, obtaining access to their devices through an external server and using a mechanism typically used by IT teams to remotely diagnose and solve problems found on employees' computers. As a result of this attack, artificial intelligence was able to identify the attacker who was trying to move around the system and access devices to encrypt files, which later turned out to be sensitive research documents of some PhD students. Thanks to the ability to identify the abnormal behavior associated with the ransomware attack, the IA immediately detected and blocked the threat accurately, without any university activity being suddenly interrupted.

The risk of a digital delay

With the growing diffusion of **eLearning** and Educational Technology, the personal data of company employees, students and school staff, the work of researchers and the very systems that make these innovative teaching methods possible are also increasingly at risk. "We are witnessing more and more attacks aimed at compromising both data integrity and the reputation of organizations, which can also jeopardize people's trust in education," says Richard Jenkins, Head of Information Risk Management, Cyber Security and Governance at International Baccalaureate. The concept expressed by this case study brings us back to opinions expressed by many in recent months: "In the future we may find ourselves in the middle of a real war between AI. An epochal clash, in which man will play a fundamental role only if he knows how to approach these ecosystems in the right way, with ethics and new digital skills". Fundamental factors on which we must focus with a solid and concrete long-term vision, to support processes and operational flows that otherwise risk perishing under the weight of a **digital divide** that could lead to a historical delay difficult to fill, in countries like Italy.

Translated with www.DeepL.com/Translator