PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4772 di Lunedì 14 settembre 2020

Difendere la privacy nell'eLearning con l'Intelligenza Artificiale

E' possibile proteggere i sistemi informatici con l'intelligenza artificiale?

Nel corso del 2020 abbiamo potuto toccare con mano quanto la **cybersecurity** sia un aspetto fondamentale di un mondo digitale.

A livello globale, abbondano le notizie di attacchi informatici a database di scuole, università, piattaforme di distance learning e collaboration. Il rischio è grave, se si pensa al valore che quelle informazioni hanno per i cybercriminali, e va gestisto e calcolato. Per comprendere meglio la situazione abbiamo approfondito l'esperienza di un'azienda statunitense operante nel settore della cyber defense basata su intelligenza artificiale. Cosa significa? In questo caso, la tecnologia di risposta agli **attacchi informatici** è autonoma e auto-apprendente.

"Si è scoperto che, nel mese di aprile, un'**università del Regno Unito** è stata colpita da un attacco ransomware, una tipologia di malware che in pochi secondi blocca l'accesso al sistema informatico pretendendo un riscatto economico in cambio del ripristino delle funzionalità. Gli hacker hanno cercato di accedere ai computer sia del personale sia degli studenti, ottenendo l'accesso ai loro dispositivi attraverso un server esterno e sfruttando un meccanismo impiegato tipicamente dai team IT per diagnosticare e risolvere a distanza i problemi riscontrati sui computer dei dipendenti. In seguito a questo attacco, l'**intelligenza artificiale** è stata in grado di individuare l'aggressore che stava cercando di spostarsi all'interno del sistema e di accedere ai dispositivi per cifrare file, che in seguito si sono rivelati essere documenti sensibili di ricerca di alcuni studenti dottorandi. Grazie alla capacità di identificare il comportamento anomalo associato all'attacco ransomware, l'IA ha immediatamente rilevato e bloccato la minaccia con precisione, senza che nessuna attività dell'università venisse improvvisamente interrotta".

Il rischio di un ritardo digitale

Con la crescente diffusione dell'**eLearning** e dell'Educational Technology, anche i dati personali dei dipendenti aziendali, degli studenti e del personale scolastico, il lavoro dei ricercatori e gli stessi sistemi che rendono possibile queste innovative modalità di insegnamento sono sempre più a rischio. "Assistiamo a un numero sempre maggiore di attacchi mirati a compromettere tanto l'integrità dei dati quanto la reputazione delle organizzazioni e che possono quindi mettere a rischio anche la fiducia dei cittadini nel mondo dell'istruzione", commenta Richard Jenkins, Head of information Risk Management, Cyber Security and Governance presso l'International Baccalaureate. Il concetto espresso da questo caso di studio ci riporta a opinioni espresse da molti in questi mesi: "In futuro potremmo ritrovarci nel bel mezzo di una vera e propria guerra tra AI. Uno scontro epocale, nel quale l'uomo avrà un ruolo fondamentale solo se saprà approcciare questi ecosistemi nella maniera giusta, con etica e nuove competenze digitali". Fattori fondamentali su cui bisogna puntare con una visione solida e concreta di lungo periodo, per supportare processi e flussi operativi che altrimenti rischiano di perire sotto il peso di un **digital divide** che potrebbe portare a un ritardo storico difficilmente colmabile, in paesi come l'Italia.
