NOVA24 Il Sole 24 Ore 12 MARZO 2026

Cybersecurity, parola d'ordine: automatizzare e semplificare

Sicurezza. Helmut Reisinger, ceo a livello Emea di Palo Alto Networks, delinea le strategie aziendali ora che i sistemi sono basati su agenti di intelligenza artificiale e prendono decisioni

Gianni Rusconi

Partiamo da un concetto ormai noto: l'intelligenza artificiale sta assumendo sempre più il ruolo di infrastruttura critica, comparabile per importanza a energia e semiconduttori, in un contesto in cui la competizione tra Paesi e sistemi industriali non dipende da un singolo fattore. «Accesso ai dati, capacità di calcolo, capitale umano e supply chain sono tutti elementi fondamentali e, soprattutto, sono interdipendenti fra di loro», spiega Helmut Reisinger, Ceo a livello Emea di Palo Alto Networks. Lo abbiamo incontrato in anteprima a Milano per l'evento "Ignite On Tour" dell'azienda di cybersecurity californiana dedicato ai clienti e ai partner e al Sole 24 Ore ha confermato come l'AI stia attraversando una nuova fase evolutiva. Dopo la stagione del machine learning e quella più recente degli strumenti generativi, si sta affermando quella che viene definita "production AI", e quindi sistemi basati su agenti digitali capaci di eseguire attività operative e transazionali.

Detto che un'avanzata infrastruttura di calcolo può non bastare se mancano dati su cui lavorare (e talenti che sanno gestirli), la corsa in avanti dell'intelligenza artificiale eleva sempre di più la centralità della sicurezza quale fattore abilitante. «Avere una buona cybersecurity per l'Ai è importante quanto avere l'Ai stessa», ha sottolineato in proposito Reisinger, ricordando come serva ragionare su due dimensioni - l'Ai per la sicurezza e la sicurezza per l'Ai - e come in Palo Alto si utilizzino tecniche di machine learning già dal 2014, anticipando una tendenza oggi inevitabile, ovvero sia l'automazione della difesa informatica. L'Ai rende gli attacchi più veloci, scalabili e

sofisticati e l'esplosione dei dati, accelerata dal cloud e dalla stessa AI, rende impossibile gestire la sicurezza solo con interventi umani.

Gli hacker, in altre parole, utilizzano su larga scala strumenti automatizzati e AI e questo rende inefficace qualsiasi risposta tardiva. «Non si può individuare un problema sei giorni dopo – ammonisce il manager - servono rilevamento e risposta in tempo reale». È proprio anche grazie agli algoritmi, infatti, che la compagnia americana è in grado ogni giorno di analizza oltre 15 petabyte di informazioni provenienti da fonti diverse (reti, ambienti cloud, endpoint, firewall, dispositivi e sistemi industriali) e processare gli interventi post incidente attraverso la propria divisione specializzata di *threat intelligence e incident response* Unit 42. Se questo è lo scenario ben conosciuto agli addetti, c'è un'altra tendenza che ancora preoccupa. Come ha ricordato ancora Reisinger citando alcuni dati ripresi in un paper elaborato dalla Stanford University, solo una piccola parte delle implementazioni di AI (circa il 6%) è accompagnata da una strategia di sicurezza adeguata. «Molte organizzazioni – ha spiegato Reisenger - stanno adottando questa tecnologia senza proteggerla ed è lo stesso fenomeno che in passato chiamavamo shadow IT, mentre oggi parliamo di shadow AI».

La cybersecurity – ha rimarcato il Ceo - è prima di tutto un problema di dati e limitare la difesa informatica a dati locali è inefficace, perché le imprese sono interconnesse e operano su mercati globali, e l'intelligence sulle minacce deve avere la stessa dimensione. Non è un caso, quindi, che il tema della resilienza di un'organizzazione e la sua capacità di resistere agli attacchi sia ormai una priorità dei vertici aziendali (vale per tutti i settori, banking in testa) e che tale sensibilità sia rafforzata anche dal quadro normativo europeo, dal Gdpr alla direttiva Nis2 fino all'Ai Act. Per le imprese la sfida è quindi duplice: difendere infrastrutture digitali sempre più complesse e allo stesso tempo semplificare la gestione della sicurezza. Non è raro, infatti, che una grande azienda abbia accumulato negli anni decine di soluzioni diverse (Palo Alto ne calcola in media tra le 30 e le 40) e non perfettamente comunicanti fra di loro, creando di conseguenza inevitabili punti di vulnerabilità. La risposta a questo problema, secondo Reisinger, è la "piattaformizzazione" della cybersecurity, e cioè un approccio unificato alla sicurezza che nasce dall'utilizzo di piattaforme integrate e che porta anche a un cambiamento nel modo di valutare il ritorno degli investimenti, attraverso tre fattori: la protezione in tempo reale, l'automazione spinta resa possibile dell'Ai e (per l'appunto) la semplificazione a livello tecnologico.

In parallelo alla diffusione dell'AI in azienda, cresce la rilevanza della sovranità digitale. Sempre più governi e intere filiere industriali stanno cercando di controllare il flusso delle informazioni oltre i propri confini, dando vita a una forma di "nazionalismo dei dati" che rischia di frammentare l'ecosistema digitale globale. Non di meno, il perdurare delle tensioni geopolitiche stanno rendendo il cyberspazio un terreno sempre più frequentato nella competizione tra Stati. Attività di spionaggio e operazioni di sabotaggio digitale sono la punta dell'iceberg di quelli che vengono

definiti "attacchi sponsorizzati da Stati", un fenomeno in aumento e ormai parte integrante delle strategie di guerra ibrida. Solo nel 2025, Palo Alto ha monitorato circa 200 gruppi direttamente o indirettamente riconducibili a governi nazionali. «Molti attacchi – ha concluso Reisinger – mirano ad interrompere l'operatività delle imprese, altri puntano a sottrarre proprietà intellettuale o ad accumulare dati che potranno essere decifrati in futuro, quando le tecnologie quantistiche renderanno vulnerabili gli attuali sistemi di cifratura».