Pmi, ecco come usare l'intelligenza artificiale contro i software maligni

Ai. Acronis: attacchi aumentati del 293% nel primo semestre di quest'anno rispetto al 2023. Per difendersi vanno utilizzati dati e machine learning

Gianni Rusconi

Il bollettino è di quelli che non lasciano dormire tranquilli: anche il "Cyber Threat Report 2024" di Acronis, relativo alle minacce digitali del primo semestre dell'anno, conferma la tendenza all'aumento sostanziale degli attacchi malware con un dato che desta impressione, vale a dire la crescita del 293% rispetto allo stesso periodo del 2023 delle offensive sferrate tramite e-mail. Sotto osservazione sono finiti oltre un milione di singoli endpoint Windows distribuiti in 15 paesi del mondo (i Paesi più colpiti nel primo trimestre sono Bahrain, Egitto e Corea del Sud) e lo scenario che ne è emerso registra in primis la nascita di nuovi gruppi ransomware.

Una decina quelli intercettati da gennaio a marzo e i più importanti - LockBit, Black Basta e Play - sono responsabili di oltre un terzo degli oltre mille casi di attacchi rilevati, in rialzo del 23% rispetto a 12 mesi fa. Assai esplicito è anche l'uso sempre più diffuso dell'intelligenza artificiale generativa e dei modelli linguistici di grande formato da parte dei cybercriminali e non meno evidenti sono lo stato di allerta che grava sulle piccole e medie imprese, in particolare in settori critici come quelli governativo e sanitario, e i rischi a cui sono continuamente esposti i managed service provider fra azioni di phishing, tecniche di social engineering e violazioni dei sistemi di supply chain.

Il ruolo giocato dall'AI e dai modelli Llm è l'altro lato della stessa medaglia: la tecnologia (assunto già noto) non è solo uno strumento di difesa ma anche un'arma in mano ai malintenzionati, e lo provano gli attacchi che prevedono l'impiego di deepfake per la compromissione delle e-mail aziendali e annesse estorsioni, l'elusione delle cosiddette verifiche Kyc (Know Your Customer), la produzione e l'esecuzione di script e l'iniezione di codice malevolo nei processi aziendali. I ricercatori di Acronis, nello specifico, hanno individuato due tipologie di minacce riconducibili all'intelligenza artificiale, una più "soft" che sfrutta le capacità degli algoritmi per creare il malware e una seconda più impattante che incorpora l'Ai nel funzionamento del malware stesso.

Cosa quindi fare, concretamente, per evitare che l'infrastruttura aziendale (reti, dati, applicazioni, device) cada sotto i colpi dei cybercriminali? E quali le strategie che le Pmi possono adottare per contrastare gli attacchi basati sulla Gen AI?