Cos’è lo zero-day e perché l’allarme Bce sull’AI del cybercrimine arriva tardi: il rischio del blackout globale **di Redazione Economia**

Lo zero-day (la vulnerabilità sconosciuta che consente di colpire sistemi prima ancora che esista una correzione) sta diventando commodity

(Fonte: https://www.corriere.it/ 22 maggio 2026)

L’intelligenza artificiale non rappresenta più una minaccia futura per la cybersicurezza globale. È già diventata uno strumento operativo nelle mani degli attaccanti. **E il vero problema, oggi, non è tanto l’esistenza di modelli avanzati come Mythos, quanto la velocità con cui capacità offensive un tempo riservate a governi e gruppi di cybercriminali stanno diventando accessibili a chiunque**. È il messaggio lanciato da Giovanni Alberto Falcione, chief technology officer di Exein, una delle realtà italiane più avanzate nel mondo della cybersecurity (ne abbiamo scritto qui avendo raccolto più di 100 milioni da investitori istituzionali), commentando l’allarme della Bce sui rischi legati all’uso criminale dei modelli di AI generativa (ne abbiamo scritto qui).

Attività di attacco in poche ore

Il punto centrale è che la rivoluzione è già avvenuta, ma le istituzioni continuano a descriverla come uno scenario futuro. **«L’allarme della Bce arriva in ritardo», spiega il manager, «non perché sia esagerato, ma perché tratta come futura una trasformazione che è già realtà».** Negli ultimi due anni operazioni altamente specialistiche come reverse engineering, fuzzing assistito, automazione delle exploit chain o decodifica di patch software hanno subito un’accelerazione

radicale grazie ai large language model. **Attività che prima richiedevano settimane di lavoro e team di esperti oggi possono essere eseguite in poche ore** da un singolo operatore con strumenti AI disponibili sul mercato.

Diminuisce il costo tecnico dell'attacco

È un cambio di paradigma che sta demolendo una delle storiche barriere della cybersecurity offensiva: **il costo tecnico dell'attacco.** Lo zero-day — la vulnerabilità sconosciuta che consente di colpire sistemi prima ancora che esista una correzione — non è più un'arma esclusiva di intelligence statali o gruppi cyber sponsorizzati dai governi. **Sta diventando una commodity. «Mythos non è una svolta», osserva Falcione, «ma il titolo di prima pagina di una storia che chi lavora nella sicurezza dei dispositivi vede accadere da mesi».** Il nodo, quindi, non è soltanto tecnologico ma soprattutto industriale e sistemico. Ogni mese cresce il numero di vulnerabilità divulgate pubblicamente e, contemporaneamente, aumenta l'asimmetria tra chi attacca e chi difende. **Gli attaccanti possono sfruttare l'automazione offerta dai modelli AI per produrre exploit su scala** e a velocità incompatibili con i tradizionali processi di difesa.

I modelli classici non sono più attuali

I modelli classici della sicurezza informatica — scan periodici, audit annuali, patch management reattivo — non sono più sufficienti. **«Nessun team di security, per quanto finanziato, può tenere il passo con un avversario che genera exploit alla velocità di un LLM», sostiene il manager.** Per questo, la cybersicurezza dovrà spostarsi sempre più verso sistemi di protezione runtime, monitoraggio comportamentale continuo e capacità di reazione in tempo reale direttamente sui dispositivi in produzione. La partita, insomma, non si giocherà più solo nel ciclo di sviluppo software, ma "sul campo", mentre l'attacco è in corso.

Il nodo open source

C'è poi un altro elemento che, secondo Falcione, rischia di essere sottovalutato dalle autorità europee: il ruolo dell'open source. **Nel dibattito internazionale, l'attenzione si concentra spesso sui grandi operatori dell'AI come Anthropic,** accusati di sviluppare modelli sempre più potenti e potenzialmente utilizzabili anche per attività offensive.