

Primo Piano - *Cybersicurezza, l'allarme dell'Acn sui sistemi di intelligenza artificiale autonoma: "Gravi rischi, i criminali li usano per colpire su larga scala"*

Roma - 24 nov 2026 (Prima Notizia 24) **Rilevate campagne di compromissione automatizzate basate su modelli capaci di pianificare attività ed eseguire operazioni senza intervento umano. Tra le contromisure indicate agli enti e alle imprese figurano l'aggiornamento immediato delle reti esposte, la limitazione dei privilegi d'accesso e il controllo continuo delle anomalie.**

Massima allerta sulla cosiddetta intelligenza artificiale "agentica", ovvero quei sistemi autonomi in grado non soltanto di elaborare testi, ma anche di pianificare attività complesse, dialogare con i gestionali aziendali, consultare banche dati ed eseguire operazioni sul campo senza supervisione diretta. Se da un lato questa evoluzione offre notevoli margini di efficienza, dall'altro espone aziende, enti pubblici e infrastrutture strategiche a minacce inedite e particolarmente insidiose. A lanciare l'allarme è l'Agenzia per la cybersicurezza nazionale, che ha già individuato vere e proprie campagne di intrusione informatica condotte tramite agenti automatizzati. "Faccio appello agli amministratori delegati e all'alta dirigenza pubblica e privata: il debito tecnologico digitale non è più sostenibile e può diventare fatale con uno scenario di attacco mutato, come stiamo osservando, con l'IA 'agentica'", avverte il direttore generale dell'Acn, Andrea Quacivi, annunciando che l'ente diffonderà quotidianamente indicazioni tecniche e operative per contrastare queste offensive. Secondo i tecnici dell'Agenzia, le incursioni affidate a sistemi autonomi si distinguono per l'estrema rapidità di esecuzione, la capacità di operare senza sosta e il conseguente ampliamento della superficie esposta agli attacchi, fattori che scardinano i tradizionali modelli di gestione del rischio e impongono una revisione profonda delle procedure di difesa. In un simile contesto non è più tollerabile l'accumulo di quel "debito tecnologico" rappresentato da aggiornamenti rinviati, manutenzioni mancate, apparati obsoleti, falle non sanate e configurazioni inadeguate. I monitoraggi confermano, infatti, che i cybercriminali stanno già sfruttando a fini offensivi architetture agentiche come Artex per automatizzare la scelta degli strumenti di intrusione, colpire contemporaneamente su vasta scala e sfruttare in tempi record le vulnerabilità critiche scovate dalla stessa intelligenza artificiale. Per arginare l'offensiva, l'Acn ha tracciato un preciso piano di mitigazione rivolto a imprese, amministrazioni pubbliche e gestori di servizi essenziali, consultabile nel dettaglio sul portale istituzionale dell'Agenzia. Gli esperti raccomandano innanzitutto di aggiornare, isolare o scollegare al più presto tutti i sistemi esposti privi delle ultime protezioni disponibili, mettendo contemporaneamente al sicuro le interfacce di gestione attraverso il censimento degli apparati visibili in rete e lasciando accessibili all'esterno esclusivamente i servizi strettamente indispensabili. Sul fronte degli accessi viene chiesto di blindare identità e

credenziali applicando rigorosamente il principio del minimo privilegio sia agli utenti sia alle applicazioni, così da circoscrivere le autorizzazioni alle sole risorse necessarie. Occorre, inoltre, ridurre l'esposizione complessiva verificando con continuità le configurazioni e le eventuali falle delle infrastrutture, proteggere le funzioni applicative imponendo tetti alla frequenza delle richieste e ai volumi delle operazioni — a partire dalle esportazioni massive di dati o dalle modifiche ai permessi — e rafforzare infine i sistemi di rilevamento per intercettare tempestivamente qualsiasi anomalia comportamentale.

(Prima Notizia 24) Martedì 24 Novembre 2026