Cyberattacchi in Italia, l’ACN segnala l’impiego dell’intelligenza artificiale agentica

Data: Invalid Date | Autore: Redazione



Gli agenti di IA possono automatizzare diverse fasi di un attacco informatico e aumentare velocità e capacità operative dei criminali. L’Agenzia per la cybersicurezza nazionale invita imprese e pubbliche amministrazioni a intervenire sulle vulnerabilità e sui sistemi non aggiornati.

25 novembre 2026

L’**intelligenza artificiale agentica** entra negli scenari delle campagne di **cyberattacco**. A differenza di un sistema che si limita a generare testi o rispondere a domande, un agente autonomo può pianificare attività, interagire con software aziendali e database e svolgere operazioni con un intervento umano ridotto.

Secondo quanto rilevato dall’**Agenzia per la cybersicurezza nazionale (ACN)**, queste capacità possono essere sfruttate anche nelle campagne di compromissione informatica. Il direttore generale **Andrea Quacivi**ha rivolto un appello ai vertici delle organizzazioni pubbliche e private: le vulnerabilità accumulate nel tempo non possono più essere trascurate e devono essere affrontate con urgenza.

Come l’IA agentica può rafforzare gli attacchi informatici

Gli agenti autonomi possono analizzare sistemi e configurazioni, individuare punti deboli e collegare

vulnerabilità diverse per costruire percorsi d'attacco più articolati. Possono inoltre adattare le proprie attività in base alle circostanze e, in alcuni casi, generare codice malevolo per tentare di aggirare le difese.

L'automazione può rendere le operazioni **più rapide e scalabili**, ampliando le possibilità anche per gruppi con risorse o competenze limitate. Per le organizzazioni, questo significa dover considerare attacchi capaci di procedere con maggiore continuità e di sfruttare più debolezze in sequenza.

Il debito tecnologico aumenta l'esposizione

Il rischio cresce quando reti e applicazioni utilizzano componenti obsoleti, aggiornamenti rinviati o configurazioni non più adeguate. Questo accumulo di interventi mancati è spesso definito **debito tecnologico**e può lasciare aperte vulnerabilità che gli attaccanti sono in grado di individuare e sfruttare.

L'ACN richiama quindi imprese, enti pubblici e operatori di servizi essenziali a rafforzare le difese senza aspettare che si verifichi un incidente. La protezione non dipende soltanto dall'acquisto di nuovi strumenti: richiede anche inventari aggiornati dei sistemi, manutenzione costante e controllo degli accessi.

Le misure indicate per ridurre i rischi

Tra le principali azioni di mitigazione rientrano:

- **Aggiornare tempestivamente** i sistemi esposti e applicare le versioni di sicurezza disponibili. Quando non è possibile intervenire subito, valutare la segregazione o la disconnessione dei sistemi vulnerabili.
- **Limitare l'accesso alle interfacce di gestione**, mantenendo pubblici soltanto i servizi indispensabili e censendo gli asset raggiungibili da Internet.
- **Proteggere account e credenziali** applicando il principio del minimo privilegio: ogni identità, umana o applicativa, dovrebbe poter accedere soltanto alle risorse necessarie.
- **Ridurre la superficie di attacco** verificando con continuità vulnerabilità, configurazioni e servizi attivi nelle applicazioni e nelle infrastrutture.
- **Imporre limiti alle operazioni**, come la frequenza delle richieste e i volumi di dati elaborati o trasferiti, così da contenere attività anomale.

La diffusione di strumenti di **IA agentica**rende quindi ancora più importante intervenire sulle basi della sicurezza informatica. Per aziende e amministrazioni, aggiornare i sistemi, proteggere le identità digitali e controllare ciò che è esposto online sono passaggi essenziali per ridurre il rischio di compromissione.

Articolo scaricato da www.infooggi.it
https://www.infooggi.it/articolo/cyberattacchi-in-italia-l-acn-segnala-l-impiego-dell-intelligenza-artificiale-agentica/158774