LA NUOVA BUSSOLA QUOTIDIANA
DOMENICA
Direttore Riccardo Cascioli

cyber security

Il crimine informatico è servito, truffe più facili con l'AI

ATTUALITà 13_09_2025

Daniele Ciacci

L'intelligenza artificiale sta trasformando radicalmente il panorama del crimine informatico, rendendo accessibili a chiunque truffe sofisticate che fino a pochi anni fa richiedevano competenze tecniche avanzate. Il report di Anthropic dello scorso mese sui

cyberattacchi AI-assistiti documenta per la prima volta operazioni criminali completamente automatizzate, mentre l'Italia registra un aumento del 70% delle truffe online e danni per 181 milioni di euro nel solo 2024.

L'analisi dei casi emersi rivela una democratizzazione preoccupante: criminali senza competenze tecniche utilizzano l'AI per orchestrare attacchi complessi che tradizionalmente richiedevano team specializzati e anni di formazione. Ora, non si tratta di condannare acriticamente qualunque innovazione, sia chiaro, bensì di comprendere come la stessa tecnologia che promette progressi straordinari possa diventare un'arma nelle mani sbagliate.

Quando l'AI diventa complice del crimine. Il caso più emblematico documentato da Anthropic è l'operazione "Vibe Hacking": un singolo criminale, assistito dall'intelligenza artificiale Claude, è riuscito a compromettere 17 organizzazioni in un mese, dalla sanità alla difesa, con richieste di riscatto tra 75.000 e 500.000 dollari. L'AI non si limitava a fornire consulenze tecniche, ma gestiva autonomamente la scansione di migliaia di endpoint vulnerabili, sviluppava malware personalizzati e calcolava persino la capacità finanziaria delle vittime per ottimizzare le richieste di riscatto. Le barriere tecniche che proteggevano la società dai crimini informatici sofisticati si stanno sgretolando.

Anche gli operatori nordcoreani sfruttano l'AI per superare le sanzioni internazionali: lavoratori IT senza competenze informatiche di base riescono a sostenere colloqui tecnici per aziende Fortune 500, generando centinaia di milioni di dollari annui per il regime attraverso stipendi occidentali.

L’Italia non è immune da questa ondata. I casi più eclatanti del 2024-2025 mostrano una sofisticazione crescente: deepfake dell'amministratore delegato di ENI utilizzati per promuovere investimenti fraudolenti, la clonazione della voce del ministro Crosetto per estorcere un milione di euro a Massimo Moratti e altri imprenditori di primo piano, falsificazioni del governatore Panetta che hanno spinto Banca d'Italia a emettere ripetuti avvisi pubblici.

Negli Stati Uniti, l'FBI documenta 1,3 miliardi di dollari persi nel 2024 solo per romance scam, mentre il caso della multinazionale di ingegneria Arup – 25 milioni di dollari sottratti attraverso una videochiamata con dirigenti deepfake – dimostra che nemmeno le aziende più sofisticate sono al sicuro.

Come sempre, quando si tratta di normare, l’Europa è tra i primi al mondo. L'AI Act, entrato in vigore ad agosto 2024, introduce obblighi stringenti di cybersecurity per i

sistemi ad alto rischio e marking obbligatorio per i contenuti deepfake. L'Italia va oltre: il DDL sull'intelligenza artificiale, approvato dal Senato a gennaio 2025, introduce il primo reato specifico di deepfake al mondo, con pene da 1 a 5 anni di reclusione.

Gli esperti concordano: la chiave è l'educazione digitale combinata con protocolli di verifica robusti. Come suggerisce Rob Greig, CIO di Arup, dopo l'attacco subito: «Dobbiamo iniziare a mettere in dubbio quello che vediamo».

Bisogna bilanciare innovazione e sicurezza. La sfida del prossimo futuro sarà preservare i benefici dell'AI proteggendoci dai suoi abusi. Le previsioni di Deloitte parlano di 40 miliardi di dollari in frodi AI-abilitate entro il 2027, ma la stessa tecnologia che genera il problema può offrire soluzioni: sistemi AI dedicati alla cybersecurity rilevano minacce il 60% più velocemente, mentre algoritmi di machine learning identificano pattern comportamentali sospetti in tempo reale.

L'intelligenza artificiale non è un nemico, ma uno strumento che richiede governance responsabile. Non è detto che la democratizzazione del crimine informatico sia un fenomeno irreversibile, ma sicuramente chiede in risposta un approccio coordinato che combini innovazione tecnologica, regolamentazione intelligente e consapevolezza digitale diffusa. Il futuro dipenderà dalla nostra capacità di essere più veloci e intelligenti dei criminali che sfruttano la stessa tecnologia.