

Nell'ultimo anno il 40% delle imprese italiane ha subito un attacco informatico: l'indagine di Cisco

2025-05-21 09:35:35 di Forbes.it

URL:<https://forbes.it/2025/05/21/negli-ultimi-il-40-delle-imprese-italiane-ha-subito-un-attacco-informatico-lindagine-di-cisco/>

In Europa solo il 3% delle aziende ha raggiunto un livello maturo sul versante della **sicurezza informatica**, mentre il 70% si trova ancora in una fase iniziale o formativa. Questo quanto emerge dall'ultimo rapporto di Cisco attraverso il [Cybersecurity Readiness Index 2025](#). L'intelligenza artificiale è di fondamentale importanza: appena un anno fa era un elemento marginale nell'agenda di Cisco, oggi è al centro della strategia difensiva e, allo stesso tempo, rappresenta una potenziale vulnerabilità. Cinque i pilastri fondamentali che lo studio di Cisco valuta: identity intelligence, machine trustworthiness, network resilience, cloud reinforcement e Ia fortification, a cui viene aggiunta l'adozione di **31 soluzioni tecnologiche per classificare le imprese in quattro livelli di preparazione**. Ma in realtà i punti da chiarire e da analizzare sono tanti. Primo fra tutti il fatto che **i criminali informatici sfruttano l'Ia generativa per creare deepfake sofisticati**, per amplificare vulnerabilità su larga scala e distribuire malware in forme sempre più innovative. E anche le stesse applicazioni di Ia sono diventate bersaglio di nuove tipologie di attacco: prompt injection, data poisoning, comportamenti imprevisti e allucinazioni nei modelli linguistici avanzati possono compromettere l'affidabilità e la sicurezza delle soluzioni basate sull'intelligenza artificiale. Particolarmente critico è il fenomeno dell'IA ombra, ovvero l'utilizzo non autorizzato di strumenti di intelligenza artificiale pubblici da parte dei dipendenti, fuori dal controllo dell'IT. Una pratica che può causare la fuga di dati sensibili, violazioni della proprietà intellettuale e l'esposizione di informazioni riservate.

La situazione in Italia

E in Italia? Stando all'analisi condotta dal colosso informatico, **il 66% considera le minacce esterne più pericolose di quelle interne**, una percezione influenzata dalle recenti tensioni geopolitiche, con campagne di attacchi DDoS orchestrate da gruppi attivisti e attori statali. Ad essere resi di mira più degli altri sono le Pmi e il settore pubblico, spesso meno preparati rispetto ad altri settori, a testimonianza di una vulnerabilità strutturale nel nostro tessuto economico. Negli ultimi 12 mesi **il 40% delle imprese italiane ha subito un attacco informatico**, mentre il 51% prevede di subire un incidente significativo entro i prossimi due anni. Solo il 15% delle aziende si dichiara pienamente fiducioso nella propria resilienza cyber, mentre il 45% delle organizzazioni gestisce più di dieci diverse tecnologie di sicurezza, segnale di una frammentazione che ostacola una difesa efficace e coordinata. Tutto questo ha ovviamente una rilevanza anche e soprattutto sul lato economico, basti pensare che ogni singola infrazione della sicurezza informatica costa fra danni diretti e indiretti in media 400mila dollari.

Solo poche aziende investono in cybersecurity

Nonostante questo **solo una piccola percentuale di aziende italiane destina più del 20% del proprio budget IT alla cybersecurity**, tendenza che riflette una cultura aziendale orientata a privilegiare l'infrastruttura fisica rispetto alla sicurezza, erroneamente percepita come secondaria. Tuttavia, con l'espansione dell'edge computing e della superficie di attacco, questo approccio sta diventando sempre meno sostenibile. Come se non bastasse, a peggiorare la situazione contribuisce la **carenza di professionisti specializzati**. L'86% delle aziende segnala infatti una forte difficoltà nel reperire personale qualificato, difficoltà che secondo il [Cybersecurity Readiness Index 2025](#) si giustifica con un livello di formazione

ancora troppo indirizzato verso discipline tradizionali, a fronte di un progresso tecnologico che richiede invece a gran voce un continuo aggiornamento delle competenze. Ognuno insomma deve fare la sua parte, e su questo fronte Cisco si trova in prima linea con un programma volto a formare gratuitamente oltre 1,5 milioni di persone in Europa entro il 2030, potenziando allo stesso tempo l'integrazione dell'IA nelle proprie soluzioni per semplificare l'analisi delle minacce, anche per operatori meno esperti.

Verso una sicurezza integrata e intelligente: la visione di Cisco

L'indagine di Cisco suggerisce che oltre ad accelerare gli sforzi in termini di formazione, **è urgente intervenire su investimenti** e governance per colmare le vulnerabilità esistenti e affrontare con determinazione una nuova era di rischi digitali sempre più sofisticati. L'Italia può contare su partner tecnologici e strategici pronti a contribuire significativamente al cambiamento necessario per affrontare il futuro digitale con maggiore sicurezza. Cisco sta promuovendo una visione in cui la sicurezza diventa componente intrinseca dell'intera infrastruttura IT, superando la concezione di area separata per integrarsi completamente nel tessuto tecnologico aziendale. Serve quindi un approccio integrato, orchestrato e potenziato dall'intelligenza artificiale. Innovazioni come il modello "[Hybrid Mesh Firewall](#)", che incorpora elementi di sicurezza in ogni nodo della rete, rappresentano un cambio di paradigma: una sicurezza distribuita e resiliente, capace di adattarsi a uno scenario di minacce in continua evoluzione. Le aziende dovranno necessariamente **riequilibrare i propri investimenti** per proteggere adeguatamente le innovazioni basate sull'IA. Cisco si propone come guida in questa transizione, anche grazie all'integrazione di tecnologie avanzate come [AI Defense](#), specificatamente sviluppate per la protezione dei sistemi basati sull'intelligenza artificiale. **LEGGI ANCHE:** [Cisco lancia un fondo da un miliardo di dollari dedicato all'IA](#)