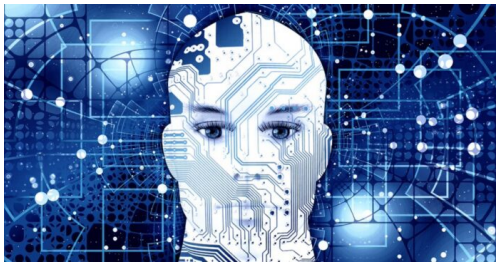

Tecno - *Cybersecurity, allarme di Deloitte sull'IA: in Italia boom di applicazioni nelle aziende, ma l'86% non ha budget per proteggersi*

Roma - 08 giu 2026 (Prima Notizia 24) **L'indagine di Deloitte e CSA rivela che molte aziende italiane ignorano i rischi della GenAI, con scarse misure di sicurezza e investimenti limitati.**

La rapida introduzione degli strumenti di intelligenza artificiale generativa all'interno del tessuto produttivo italiano non viaggia di pari passo con la predisposizione di adeguate barriere difensive, esponendo le imprese a pesanti vulnerabilità informatiche. È lo scenario delineato dall'indagine intitolata "Lo stato della GenAI Security in Italia", condotta dagli analisti di Deloitte in collaborazione con la Cloud Security Alliance (CSA), monitorando le risposte di oltre cento manager della sicurezza e grandi organizzazioni attive nel panorama nazionale. Il dossier mette in luce come quasi i due terzi delle realtà intervistate navighino ancora in assenza di un piano strutturato per la sicurezza dei sistemi algoritmici, mentre una quota infinitesimale, pari ad appena il 9%, dichiara di aver completato l'integrazione di una strategia dedicata. Il livello di maturità dei processi aziendali appare ancora più critico se si analizzano i modelli organizzativi: solo un esiguo 3% del campione esibisce un'infrastruttura matura sia sotto il profilo della governance interna sia dal punto di vista operativo. Un ulteriore elemento di criticità emerso dalla ricerca riguarda la scarsa tracciabilità dei programmi in uso. Meno di un Chief Information Security Officer (Ciso) su dieci ha infatti il pieno controllo e la visibilità totale sulle applicazioni di intelligenza artificiale effettivamente impiegate dai dipendenti nei vari reparti. Questa mancanza di monitoraggio favorisce il proliferare della cosiddetta "shadow AI" — l'utilizzo di software non autorizzati dai vertici —, che si posiziona in cima ai timori dei responsabili della sicurezza insieme al pericolo di esfiltrazione di dati riservati e alle violazioni delle normative sulla privacy. Al contrario, i manager italiani tendono ancora a sottostimare i rischi legati alle alterazioni dei modelli, ai pregiudizi dei database (bias) e alle risposte errate fornite dagli algoritmi (allucinazioni). Le note dolenti toccano anche il portafoglio aziendale, dato che ben l'86% delle imprese non ha stanziato un fondo economico specifico per blindare la sicurezza della GenAI. Nei rari casi in cui sono presenti investimenti mirati, i canali di spesa assorbono una quota marginale, compresa tra il 2% e il 3% dei finanziamenti complessivi destinati alla cybersecurity. Ad azzoppare la transizione verso un utilizzo sicuro degli algoritmi intervengono la forte carenza di figure professionali con competenze verticali sul tema, la scarsa consapevolezza dei rischi reali da parte del management e i tradizionali tetti di spesa imposti dai bilanci. I vertici delle società promotrici dello studio hanno espresso forte preoccupazione per questo squilibrio strutturale. Fabio Battelli, alla guida della divisione enterprise security di Deloitte, ha rimarcato come la stragrande maggioranza delle aziende italiane affronti le minacce tecnologiche al di fuori di percorsi e regole formalizzate, lasciando scoperto il fianco a potenziali attacchi. Sulla stessa linea d'onda l'analisi di Daniele

Catteddu, chief technology officer di CSA, il quale ha identificato proprio nel divario tra la corsa all'implementazione dell'intelligenza artificiale e la capacità di controllarla una delle sfide più urgenti e complesse per il futuro dell'ordine informatico aziendale.

(Prima Notizia 24) Lunedì 08 Giugno 2026