Le aziende accelerano l'adozione di strumenti di intelligenza artificiale generativa nonostante le preoccupazioni legate alla sicurezza

- *Il 95% delle aziende sta utilizzando in qualche modo strumenti di intelligenza artificiale generativa*
- *L'89% considera gli strumenti di IA generativa un potenziale rischio per la sicurezza*
- *Il 23% di coloro che utilizzano strumenti IA generativa ammette di non aver implementato alcun tipo di controllo*
- *I team IT, e non i dipendenti, sono la forza trainante che spinge per il loro utilizzo*

Milano, 16 Novembre 2023 - Una nuova ricerca di Zscaler, Inc. (NASDAQ: ZS), leader nella sicurezza del cloud, svela come le aziende sentano fortemente la pressione nell'accelerare sull'utilizzo di strumenti di **intelligenza artificiale generativa (GenAI), nonostante i notevoli problemi di sicurezza legati al suo utilizzo**. Secondo l'ultima survey condotta sul tema intitolata "Occhi puntati sulla sicurezza della GenAI", che ha coinvolto oltre 900 Reponsabili IT a livello internazionale, sebbene **l'89% delle aziende consideri gli strumenti di GenAI come ChatGPT un potenziale rischio per la sicurezza**, **il 95% li sta già utilizzando** in qualche modo all'interno della propria azienda.

Ancora più preoccupante è il dato che rileva come **il 23% degli intervistati non stia monitorando affatto l'utilizzo** di questi strumenti e il **33% non abbia ancora implementato alcuna misura di sicurezza aggiuntiva** legata all'utilizzo della GenAI, anche se molti l'hanno pianificato. La situazione appare particolarmente evidente tra le aziende di piccole dimensioni (500-999 dipendenti), dove lo stesso numero di aziende sta utilizzando strumenti di GenAI **(95%),** ma ben il **94%** riconosce sia rischioso.

"*Gli strumenti di GenAI, tra cui ChatGPT e altri, sono molto promettenti per le aziende in termini di velocità, innovazione ed efficienza*", ha sottolineato Sanjay Kalra, VP Product Management di Zscaler. "*Tuttavia, data l'attuale poca chiarezza relativa alle misure di sicurezza, solo il **39%** delle aziende percepisce la loro adozione come un'opportunità piuttosto che come una minaccia. Questo non solo mette a rischio la loro attività e l'integrità dei dati dei clienti, ma spreca anche il loro enorme potenziale*".

Tuttavia, la pressione per l'impiego di queste tecnologie non proviene da dove si potrebbe pensare, e i risultati rivelano che l'IT sia in grado di riprendere il controllo della situazione. Nonostante la consapevolezza diffusa, non sono al momento i dipendenti la forza trainante né in termini di interesse né per quanto riguarda l'utilizzo: infatti solo il **5%** degli intervistati dichiara che la richiesta è partita dai dipendenti. Il **59%** ha invece affermato che l'utilizzo sia stato stimolato direttamente dai team IT.

"*Il fatto che i team IT siano alla guida dovrebbe rassicurare i leader aziendali*", continua Kalra. "*Significa che il gruppo dirigente ha l'autorità per regolare strategicamente il ritmo con cui adottare l'Intelligenza artificiale generativa e stabilire un preciso controllo sulle misure di*

sicurezza, prima che la sua diffusione all'interno dell'azienda progredisca ulteriormente. Tuttavia, è essenziale riconoscere che la finestra temporale per ottenere una governance sicura si sta rapidamente riducendo".

A fronte del **51%** degli intervistati che prevede un aumento significativo dell'interesse per gli strumenti di intelligenza artificiale generativa entro la fine dell'anno, le aziende devono agire rapidamente per colmare il divario tra utilizzo e sicurezza.

Ecco alcune misure che i dirigenti aziendali possono adottare per garantire che l'uso degli strumenti di intelligenza artificiale generativa nella loro azienda sia adeguatamente protetto:

- Implementare un'architettura Zero Trust globale per autorizzare solo applicazioni IA e utenti approvati.
- Eseguire valutazioni approfondite dei rischi per la sicurezza delle nuove applicazioni di IA per comprendere chiaramente e le vulnerabilità e agire di conseguenza.
- Creare un sistema di registrazione completo per tenere traccia di tutte le richieste e le risposte dell'IA.
- Attivare misure di prevenzione della perdita di dati (DLP) Zero Trust per tutte le attività di IA per proteggersi dall'esfiltrazione dei dati.

Ulteriori informazioni

https://info.zscaler.com/rs/306-ZEJ-256/images/zscaler-genai_survey_infographic.pdf

Metodologia

Nell'ottobre 2023, Zscaler ha commissionato a Sapio Research un'indagine su 901 responsabili decisionali IT (ITDM) in 10 mercati (Australia e Nuova Zelanda, Francia, Germania, India, Italia, Paesi Bassi, Singapore, Spagna, Regno Unito e Irlanda, Stati Uniti) e che lavorano in aziende con più di 500 dipendenti in diversi settori.

Sapio Research è un'agenzia di ricerche di mercato in ambito B2B e tecnologico che aiuta le aziende a crescere grazie a servizi di ricerca di alta qualità, efficienti e affidabili.

A proposito di Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange protegge migliaia di clienti da attacchi informatici e dalla perdita di dati collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata su SSE, è la più grande piattaforma di sicurezza cloud in line del mondo.

Per ulteriori informazioni:

Tania Acerbi

Monica Fecchio

Prima Pagina

Piazza Giuseppe Grandi 19 - 20129 Milano

e-mail: tania@primapagina.it

e-mail: monica@primapagina.it