Zero Trust in crescita, ma lâ??AI per la sicurezza lenta a decollare: il report DXC e Microsoft

Descrizione

(Adnkronos) â?? Unâ??analisi globale condotta da DXC Technology e Microsoft rivela un quadro a due velocitÃ nel panorama della cybersecurity aziendale: se da un lato il modello Zero Trust Ã¨ ormai un framework irrinunciabile e ampiamente adottato, dallâ??altro lâ??integrazione di strumenti di sicurezza basati sullâ??Intelligenza Artificiale (AI) procede con notevole ritardo.

Lo studio, intitolato The Trust Report: From Risk Management to Strategic Resilience in Cybersecurity, sottolinea come lâ??adozione del modello Zero Trust abbia prodotto risultati tangibili e significativi. Tra le organizzazioni intervistate, ben lâ??83% di quelle che hanno implementato questo approccio strategico ha registrato una â??significativa riduzione degli incidenti informaticiâ?•, ottenendo in parallelo un abbattimento dei costi di ripristino e assistenza.

Tale dato certifica il Zero Trust non piÃ¹ come una semplice best practice, ma come un framework essenziale per proteggere le organizzazioni da un panorama di minacce in continua evoluzioneï»¿.

La ricerca, commissionata da DXC e Microsoft, ha coinvolto oltre cento esperti di sicurezza informatica a livello globale, evidenziando che lâ??accelerazione delle minacce (anche grazie allâ??AI che offre agli hacker nuove modalitÃ per aggirare le difese) spinge le aziende a rafforzare le proprie difese.

Tuttavia, il percorso verso la piena adozione del Zero Trust non Ã¨ privo di ostacoli. I principali risultati dello studio sottolineano le sfide in essere:

Il 66% delle organizzazioni individua i sistemi legacy come la difficoltÃ maggiore nellâ??implementazione del Zero Trust.

Il 72% delle aziende dichiara che le minacce emergenti sono il fattore principale che le spinge a un miglioramento continuo delle politiche di sicurezza.

Oltre il 50% delle organizzazioni ha scoperto un beneficio inatteso nella capacitÃ del Zero Trust di migliorare lâ??esperienza utente, oltre alla sicurezza.

Nonostante lâ??AI stia alimentando una crescita esponenziale delle minacce informatiche, la sua integrazione nelle difese aziendali Ã¨ ancora agli albori. Soltanto il 30% degli interpellati ha dichiarato di utilizzare attivamente strumenti di autenticazione basati sullâ??AI per migliorare le proprie procedure di sicurezza.

Questo notevole divario tra lâ??adozione dellâ??AI da parte degli attaccanti e il suo impiego difensivo rivela un vasto â??potenziale ancora inespresso per rafforzare la cybersecurityâ?•. Lâ??Intelligenza Artificiale, infatti, puÃ² offrire una protezione piÃ¹ proattiva e adattiva contro cyber attacchi in costante trasformazione. I leader del settore sottolineano lâ??importanza di un approccio olistico e integrato. Dawn-Marie Vaughan, Global Offering Lead Cybersecurity di DXC, ha dichiarato: â??Il modello Zero Trust Ã¨ sempre piÃ¹ considerato lo standard per il futuroâ?•. E ha aggiunto: â??Con lâ??accelerazione delle minacce alimentate dallâ??intelligenza artificiale, le organizzazioni devono valutare la sicurezza con un approccio olistico, che coinvolga identitÃ , dispositivi, reti, applicazioni e datiâ?•.

Dichiarazione a cui fa eco Alex Simons, CVP, Microsoft Entra: â??La maggior parte delle aziende si affida giÃ a Microsoft Entra ID e Microsoft 365 come infrastruttura portante dei propri ambienti ITâ?•. Simons ha sottolineato che la collaborazione tra le due aziende mira ad amplificare il valore del Zero Trust, â??abilitando maggiore integrazione, operazioni semplificate, migliore visibilitÃ e controlloâ?•.

Gli esperti di DXC ribadiscono, infine, che lâ??implementazione del Zero Trust non Ã¨ unâ??azione singola, ma un â??percorso continuo che richiede cambiamento culturale, monitoraggio costante e partnership solideâ?•. Le aziende sono invitate ad adottare un approccio graduale, partendo dallâ??identitÃ e avvalendosi di partner affidabili per ottimizzare e gestire architetture su larga scala.

â??

tecnologia

webinfo@adnkronos.com (Web Info)

Categoria

1. Tecnologia

Tag

1. tec

Data di creazione
Ottobre 21, 2025
Autore
redazione