



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

Descrizione

(Adnkronos) Un'analisi globale condotta da DXC Technology e Microsoft rivela un quadro a due velocità nel panorama della cybersecurity aziendale: se da un lato il modello Zero Trust è ormai un framework irrinunciabile e ampiamente adottato, dall'altro l'integrazione di strumenti di sicurezza basati sull'Intelligenza Artificiale (AI) procede con notevole ritardo.

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

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

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

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

Il 66% delle organizzazioni individua i sistemi legacy come la difficoltà maggiore nell'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 capacità del Zero Trust di migliorare l'esperienza utente, oltre alla sicurezza.

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

Questo notevole divario tra l'adozione dell'AI da parte degli attaccanti e il suo impiego difensivo rivela un vasto potenziale ancora inespresso per rafforzare la cybersecurity. L'Intelligenza Artificiale, infatti, può offrire una protezione più proattiva e adattiva contro cyber attacchi in costante trasformazione. I leader del settore sottolineano l'importanza di un approccio olistico e integrato. Dawn-Marie Vaughan, Global Offering Lead Cybersecurity di DXC, ha dichiarato: «Il modello Zero Trust è sempre più considerato lo standard per il futuro». E ha aggiunto: «Con l'accelerazione delle minacce alimentate dall'intelligenza artificiale, le organizzazioni devono valutare la sicurezza con un approccio olistico, che coinvolga identità, dispositivi, reti, applicazioni e dati».

Dichiarazione a cui fa eco Alex Simons, CVP, Microsoft Entra: «La maggior parte delle aziende si affida già a Microsoft Entra ID e Microsoft 365 come infrastruttura portante dei propri ambienti IT». Simons ha sottolineato che la collaborazione tra le due aziende mira ad amplificare il valore del Zero Trust, «abilitando maggiore integrazione, operazioni semplificate, migliore visibilità e controllo».

Gli esperti di DXC ribadiscono, infine, che l'implementazione del Zero Trust non è un'azione singola, ma un percorso continuo che richiede cambiamento culturale, monitoraggio costante e partnership solide. Le aziende sono invitate ad adottare un approccio graduale, partendo dall'identità e avvalendosi di partner affidabili per ottimizzare e gestire architetture su larga scala.

»

tecnologia

webinfo@adnkronos.com (Web Info)

Categoria

1. Tecnologia

Tag

1. tec

Data di creazione

Ottobre 21, 2025

Autore

redazione