Il 38% delle aziende dispone dell'infrastruttura per supportare il lavoro ibrido, ma per trattenere i talenti è necessario offrire loro un'esperienza ibrida ottimizzata

- *Una ricerca di Zscaler ha rilevato che il 50% delle aziende **(53% in Italia)** che hanno spostato le applicazioni nel cloud prevede di implementare, o sta ancora implementando, un'architettura ibrida Zero Trust.*
- *Il 52% **(stessa percentuale per l'Italia),** ritiene che un'architettura Zero Trust aiuterebbe a risolvere il problema dell'incoerenza delle esperienze di accesso alle applicazioni e ai dati basati su cloud e on-premise.*
- *Il 47% **(44% in Italia)** delle aziende con un'architettura basata su VPN ritiene che sia troppo complesso amministrare una sicurezza differenziata per i dipendenti in sede e per quelli in remoto.*

Milano, 31 Marzo 2023 – L'attuale situazione del mercato del lavoro a livello globale è complessa e le aziende sono alla ricerca di modi per trattenere e attrarre nuovi talenti, offrendo la possibilità di lavorare da qualsiasi luogo, garantendo una connettività continua, consentendo esperienze digitali personalizzate e molto altro ancora. Ma solo il 39% delle aziende **(36% in Italia)** dispone dell'infrastruttura (Zero Trust o VPN) per supportare un ambiente di lavoro ibrido sicuro e un altro 35% **(27% in Italia)** non ha ancora iniziato a implementarlo o non ha intenzione di farlo. Questo è quanto emerge dall'ultima ricerca di Zscaler sullo stato della trasformazione Zero Trust, che ha raccolto le opinioni di 1.900 responsabili IT di livello senior di aziende che hanno già iniziato la migrazione di applicazioni e servizi verso il cloud.

"I dipendenti, soprattutto quelli più giovani, si aspettano sempre di più che la loro esperienza digitale durante il lavoro sia ottimizzata con, a portata di mano, un accesso alle applicazioni veloce e senza soluzione di continuità", ha dichiarato **Ismail Elmas, Global Vice President International di Zscaler**. *"Il potenziale delle soluzioni Zero Trust sta iniziando a diventare evidente sia per i responsabili IT che per quelli aziendali. Ma c'è ancora spazio per educare le aziende sul suo valore al di là della sicurezza e come fattore abilitante per il luogo di lavoro del futuro. L'implementazione di una piattaforma Zero Trust consentirà alle aziende di adattare e far evolvere facilmente il proprio modello di lavoro ibrido per ridurre gli ostacoli alla sicurezza per il personale e offrire ai dipendenti esperienze efficienti e affidabili".*

Una recente ricerca di LinkedIn ha rilevato che il 93% delle aziende a livello globale è preoccupata della fidelizzazione dei propri dipendenti. Le aziende faticano a rimanere in attivo, la stabilità è fondamentale e trattenere i talenti è oggi fondamentale più che mai. Infatti, i responsabili delle decisioni IT intervistati da Zscaler, considerano attrarre e trattenere i migliori talenti uno dei tre principali driver della trasformazione digitale **(**25%, **in Italia il 23%),** insieme alla crescita dei ricavi (22%, **in Italia il 19%**) e al supporto delle nuove strategie aziendali (24%, **in Italia il 28%).**

I dipendenti si aspettano esperienze fluide

Se da un lato le aziende sono consapevoli che trattenere i talenti è fondamentale, dall'altro molti responsabili IT riconoscono che i dipendenti vivono esperienze digitali di qualità scadente a causa dell'infrastruttura di sicurezza legacy che non è in grado di gestire il lavoro ibrido. Secondo la ricerca, il 52% **(stessa percentuale per l'Italia)** cita l'incoerenza delle esperienze di accesso alle applicazioni e

ai dati come uno dei motivi principali per cui sta cercando di implementare un'infrastruttura di lavoro ibrida basata su Zero Trust. Un altro 39% **(30% in Italia)** ritiene che l'utilizzo delle soluzioni Zero Trust consentirebbe ai dipendenti un accesso più agevole e diretto alle applicazioni e ai dati dai dispositivi personali.

L'esperienza dell'utente non è l'unica preoccupazione rilevata dalla ricerca. Gli intervistati hanno anche espresso la convinzione che l'attuale infrastruttura possa avere un impatto sulla produttività del personale. Quasi la metà (46%, **in Italia 30%)** dei responsabili IT che stanno implementando o pianificando l'implementazione di un'infrastruttura di lavoro ibrida basata sull'architettura Zero Trust lo hanno fatto perché i loro dipendenti hanno problemi di accesso con le soluzioni di sicurezza attuali e il 27% **(36% in Italia)** ha dichiarato di voler migliorare la sicurezza della connettività per la propria forza lavoro ibrida.

Ash Surti, Executive Vice President, Technology and Security di Colt Technology Services, ha dichiarato: *"Il lavoro flessibile è un elemento importante per attrarre talenti, ma allo stesso tempo il lavoro da remoto amplia la superficie di attacco, presentando rischi e complessità per i team IT incaricati di offrire un'esperienza omogenea e coerente in tutta l'infrastruttura digitale. La ricerca di Zscaler riconosce questo aspetto ed evidenzia la crescente domanda di piattaforme Zero Trust, dal momento che le aziende mettono in discussione i modelli tradizionali per creare il luogo di lavoro del futuro".*

LE VPN minano la sicurezza

Molte aziende si sono già affidate alle reti private virtuali (VPN) per mantenere una rete aziendale sicura e consentire ai dispositivi personali di accedere a cartelle protette. Se un tempo questa poteva sembrare una via rapida e sicura per proteggere la rete di un'azienda, oggi il 54% **(40% in Italia)** dei responsabili IT ritiene che le VPN o i firewall perimetrali siano inefficaci per garantire la protezione dai cyberattacchi e forniscano scarsa visibilità sul traffico delle applicazioni e sugli attacchi stessi. Dal punto di vista dell'esperienza dei dipendenti, i dati suggeriscono che anche le VPN non sono la risposta adatta. Due quinti (39%) dei responsabili IT **(ma solo il 13% in Italia)** la cui azienda utilizza una VPN, affermano che i dipendenti subiscono un rallentamento delle prestazioni delle applicazioni e un terzo (33%, **in Italia il 25%)** lamenta connessioni instabili.

La ricerca di Zscaler mostra che i leader IT stanno adottando il modello Zero Trust - ovvero il principio secondo cui nessun utente o applicazione deve essere considerato intrinsecamente affidabile, nonché quello di collegare utenti alle applicazioni, e non alla rete aziendale - come soluzione necessaria per proteggere gli utenti, i workload e i dispositivi aziendali in una realtà lavorativa altamente distribuita incentrata sul cloud e sulla telefonia mobile, consentendo al contempo un coinvolgimento e un'esperienza più fluidi per i dipendenti, indipendentemente da dove si trovino.

Ulteriori informazioni

A questo link è possibile accedere al report completo *The State of Zero Trust Transformation 2023*.

Metodologia

Le conclusioni di questo report si basano sui dati raccolti nell'ambito di uno studio commissionato da Zscaler e condotto da ATOMIK Reasearch che ha intervistato 1.900 responsabili delle decisioni aziendali (CIO / CISO / CDO / Head of Network Architecture) nelle regioni EMEA (Regno Unito,

Germania, Francia, Paesi Bassi, Svezia, Italia, Spagna), AMS (USA, Messico, Brasile) e APAC (Giappone, India, Australia, Singapore). La ricerca è stata condotta nel luglio 2022. Il campione comprendeva aziende fino a 4.999 dipendenti (43%), da 5.000 a 9.999 dipendenti (32%) e da 10.000 o più dipendenti (25%).

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