Il report Zscaler sui rischi legati alle VPN rivela che quasi la metà delle aziende è preoccupata della propria sicurezza a causa dell'utilizzo di VPN non sicure

VPN, email e dispositivi dell'utente finale non sicuri sono stati identificati come principali vettori di attacco, sottolineando la necessità di un'architettura Zero Trust

- L'88% delle aziende dichiara di temere che le VPN compromettano la loro capacità di mantenere un ambiente sicuro
- Il 90% delle aziende teme che i criminali informatici possano prenderle di mira attraverso VPN di proprietà di terzi
- Anche il livello di soddisfazione degli utenti è basso, con il 72% degli utenti che esprime frustrazione a causa di connessioni VPN lente e inaffidabili

Milano, 5 settembre 2023 – Zscaler, Inc. (NASDAQ: ZS), leader nella sicurezza del cloud, ha rivelato oggi i risultati del suo report annuale sui rischi legati alle VPN, prodotto da Cybersecurity Insiders, da cui emerge che un numero impressionante di aziende esprime forti preoccupazioni per la sicurezza della rete a causa dei rischi legati alle VPN. Il report include un sondaggio condotto su 382 professionisti dell'IT e della sicurezza informatica di diversi settori ed esplora le sfide che si trovano ad affrontare in materia di sicurezza e di esperienza utente. Il report sottolinea la necessità per le aziende di rivalutare il proprio livello di sicurezza e di migrare verso un'architettura Zero Trust a causa delle crescenti minacce che sfruttano le vulnerabilità delle VPN.

"Il report evidenzia che il 92% degli intervistati riconosce l'importanza di adottare un'architettura Zero Trust; tuttavia, è preoccupante vedere che molte aziende utilizzano ancora una VPN per l'accesso remoto dei dipendenti e di terze parti, fornendo così inavvertitamente un'attraente superficie di attacco per i criminali informatici", ha dichiarato Deepen Desai, Global CISO e Head of Security Research di Zscaler. "I fornitori di firewall e VPN tradizionali stanno creando VPN virtuali nel cloud definendole soluzioni Zero Trust, evitando la parola "VPN". I clienti devono porsi le domande giuste per assicurarsi che queste offerte obsolete virtualizzate nel cloud non diano loro un falso senso di sicurezza. Per proteggersi dall'evoluzione degli attacchi ransomware, è fondamentale che le aziende eliminino l'uso delle VPN, diano priorità alla segmentazione utente-applicazione e implementino un motore di prevenzione della perdita di dati contestuale in linea, con ispezione TLS completa".

Le vulnerabilità VPN sottolineano la necessità di un'architettura Zero Trust

L'88% delle aziende esprime profonda preoccupazione per le potenziali violazioni dovute alle vulnerabilità delle VPN. In particolare, le aziende sono più preoccupate per i possibili attacchi di phishing (49%) e di ransomware (40%) come conseguenza del regolare utilizzo delle VPN.

Quasi la metà delle aziende ha dichiarato di essere stata presa di mira da criminali informatici in grado di sfruttare una vulnerabilità della VPN, come protocolli obsoleti o fughe di dati, e una su cinque ha subito un attacco nell'ultimo anno. Il ransomware, in particolare, è emerso come un avversario significativo per le aziende, con il 33% vittima di attacchi ransomware su VPN nell'ultimo anno.

Gli utenti di terze parti sono una delle principali preoccupazioni
Nonostante le diligenti misure di sicurezza, la ricerca mostra che il 90% delle aziende è ancora molto preoccupato che i fornitori di terze parti possano essere sfruttati dai criminali informatici per ottenere un accesso backdoor indiretto alle loro reti. Gli utenti esterni, come collaboratori e fornitori, rappresentano un rischio potenziale per l'azienda a causa di standard di sicurezza differenti, della mancanza di visibilità sulle pratiche di sicurezza della rete e della complessità della gestione degli accessi esterni da parte di terzi.

Le architetture di rete e di sicurezza tradizionali gestiscono l'accesso alle applicazioni interne fornendo agli utenti accesso diretto alla rete - fidandosi intrinsecamente degli utenti che possono confermare le proprie credenziali al punto di accesso, il che si trasforma in un problema se tali credenziali vengono rubate. Grazie all'approccio Zero Trust, gli utenti si collegano direttamente alle applicazioni e alle risorse di cui hanno bisogno, mai alle reti. Le connessioni da utente ad applicazione e da applicazione ad applicazione eliminano il rischio di spostamenti laterali e impediscono ai dispositivi compromessi di infettare altre risorse. Inoltre, gli utenti e le applicazioni sono invisibili a Internet, quindi non possono essere scoperti o attaccati.

Un'esperienza utente insoddisfacente può portare a problemi di sicurezza
Oltre ai problemi di sicurezza, il 72% degli utenti è insoddisfatto della propria attuale esperienza con le reti VPN a causa di connessioni lente e inaffidabili. In particolare, il 25% è frustrato dalla lentezza delle applicazioni, mentre il 21% deve affrontare frequenti interruzioni della connessione.

L'inaffidabilità della connettività Internet contribuisce a un'esperienza negativa per gli utenti, causando frustrazione e un minore coinvolgimento degli stessi. Inoltre, la complessità dell'autenticazione può portare a una produttività ridotta, a un calo dei ricavi e a un aumento del rischio di perdita di dati da parte degli utenti che trovano il modo di aggirare servizi VPN inefficienti.

Il passaggio a Zero Trust
Le aziende che si rendono conto del ruolo delle VPN obsolete nel creare questi problemi in termini di sicurezza ed esperienza utente stanno iniziando a migrare verso un'architettura Zero Trust. Infatti, il 92% riconosce l'importanza di adottare un approccio Zero Trust per salvaguardare le proprie risorse e i propri dati, con un aumento del 12% rispetto all'anno precedente, mentre il 69% sta già pianificando la sostituzione delle VPN attuali con soluzioni Zero Trust Network Access (ZTNA).

Mitigazione dei rischi legati alle VPN grazie all'architettura Zero Trust
Il report raccomanda alle aziende di implementare un'architettura Zero Trust per mitigare in modo efficace i rischi associati alle vulnerabilità delle VPN e proteggere i loro dati e applicazioni sensibili dagli attacchi informatici.

- Per maggiori informazioni sulle best practice per migrare dalle VPN, consultare l'articolo del blog *New VPN Risk Report: Third-Party Access Identified as a Huge Risk to Organizations*

- Per scaricare il report 2023 sui rischi legati alle VPN di Zscaler, visitare il sito https://info.zscaler.com/2023-vpn-risk-report
- Per indicazioni su come sostituire la rete VPN, è disponibile l'eBook *Securing Your Hybrid Workforce with ZTNA*.

Metodologia

Il report 2023 Zscaler sui rischi legati alle VPN di Zscaler si basa sul sondaggio condotto tra 382 professionisti IT ed esperti di sicurezza informatica e prende in esame queste complesse sfide legate alla sicurezza e all'esperienza utente. Il report di quest'anno rivela la complessità dell'attuale gestione delle VPN, i problemi legati all'esperienza dell'utente, le vulnerabilità a diversi attacchi informatici e il loro potenziale di violazione del livello di sicurezza delle aziende in senso più ampio.

A proposito di Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. 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