Il nuovo rapporto sui rischi delle VPN di Zscaler evidenzia i rischi di sicurezza nascosti che colpiscono le imprese e offre alternative per l'accesso sicuro da remoto

La ricerca del 2021 evidenzia le crescenti vulnerabilità di sicurezza legate agli attacchi mirati di social engineering, ransomware e malware

Milano – 24, febbraio 2021 Zscaler, Inc. (NASDAQ: ZS), leader nella cloud security, ha annunciato oggi un nuovo studio che prende in esame le vulnerabilità nascoste rilevate nelle reti private virtuali aziendali (VPN) e mette in evidenza la necessità di un approccio di sicurezza zero-trust per mitigare le minacce. Pubblicato in collaborazione con Cybersecurity Insiders, il report include i risultati di una survey globale che ha coinvolto di più di 350 professionisti della sicurezza informatica sullo stato attuale degli ambienti di accesso remoto, l'aumento delle vulnerabilità legate alle reti VPN e il ruolo dei modelli di sicurezza zero-trust nel fornire accesso alle applicazioni aziendali. È possibile scaricare lo studio completo qui: Zscaler 2021 VPN Risk Report.

Negli ultimi tre decenni, si è diffuso l'uso delle reti VPN per consentire agli utenti di accedere da remoto alle risorse sulle reti aziendali. Tuttavia, l'aumento della domanda di soluzioni per il telelavoro, la migrazione verso il cloud e i progressi nell'ambito della trasformazione digitale, hanno fatto emergere una forte incompatibilità tra le VPN e le architetture di sicurezza realmente zero-trust. Queste incompatibilità, in gran parte dovute alla necessità intrinseca delle VPN di accedere alla rete e di essere esposte a Internet, hanno aumentato la superficie di attacco aziendale permettendo ai criminali informatici di sfruttare questi modelli legacy basati sulla fiducia intrinseca degli utenti.

Il report 2021 Zscaler VPN Risk mette in evidenza l'attuale utilizzo delle VPN da parte delle imprese e le principali sfide affrontate dagli amministratori IT che gestiscono le VPN. Suggerisce le alternative ai responsabili delle reti e della sicurezza che desiderano fornire un accesso veloce, trasparente e sicuro alle applicazioni aziendali senza compromettere le loro strategie di sicurezza zero-trust; inoltre, include dati che forniscono un'idea sul ruolo che le soluzioni zero-trust ricopriranno nel futuro dell'accesso da remoto. Di seguito i principali risultati emersi dalla survey:

- Il 93% delle aziende intervistate ha implementato servizi VPN, nonostante il 94% degli intervistati abbia ammesso di essere consapevole che i criminali informatici sfruttano le VPN per accedere alle risorse di rete.
- Gli intervistati hanno indicato che il social engineering (75%), il ransomware (74%) e il malware (60%) sono i vettori di attacco che più li preoccupano e sono spesso utilizzati per colpire gli utenti che accedono alle VPN.

- Con quasi tre imprese su quattro preoccupate per la sicurezza delle VPN, il 67% delle aziende sta prendendo in considerazione alternative di accesso remoto alla VPN tradizionale.
- Come risultato dei crescenti rischi per la sicurezza delle VPN, il 72% delle aziende sta dando priorità all'adozione di un modello di sicurezza zero-trust, mentre il 59% ha accelerato i propri progetti data la focalizzazione sul telelavoro.
- In merito alle future necessità di servizi zero-trust, il report afferma che il 77% degli intervistati ha indicato che la loro forza lavoro sarà ibrida, con una maggiore flessibilità in termini di presenza in ufficio e telelavoro.

"È incoraggiante sapere che le imprese comprendono che le architetture zero-trust presentano uno dei modi più efficaci per fornire accesso sicuro alle risorse aziendali", ha affermato Chris Hines, Director, Zero Trust Solutions di Zscaler. "Nel proseguire con il loro percorso di migrazione verso il cloud e il supporto ad una nuova forza lavoro ibrida, le aziende dovrebbero ripensare la loro strategia di sicurezza e valutare le crescenti minacce per la cybersecurity che stanno attivamente sfruttando le tradizionali soluzioni di accesso remoto, come le VPN. L'approccio più sicuro è quello di portare gli utenti in modo sicuro e diretto alle applicazioni, intermediando tutte le connessioni utente-applicazioni utilizzando un servizio di accesso zero-trust fornito in cloud".

I risultati completi del report Zscaler VPN Risk sono disponibili sulla pagina dedicata VPN Risk Report 2021.

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, basato su SASE, è la più grande piattaforma di sicurezza cloud in line del mondo.

Zscaler™ and the other trademarks listed at https://www.zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

.

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
Tel. +39 02 91339811