Report del 2023 sui rischi della VPN

Cybersecurity INSIDERS

Panoramica

Le reti private virtuali (VPN) vengono impiegate da molto tempo per facilitare l'accesso remoto di base. Tuttavia, la rapida crescita della forza lavoro distribuita e la sempre maggiore adozione delle tecnologie cloud stanno mettendo in discussione il tipo di connettività che offrono.Di fronte a una panorama di minacce in costante evoluzione, le VPN si rivelano infatti inefficaci nel supportare l'accesso sicuro e segmentato di cui le organizzazioni hanno bisogno. Al contrario, spesso forniscono un accesso totale alla rete aziendale, incrementando di conseguenza le possibilità di subire attacchi informatici nel caso in cui gli utenti malintenzionati riuscissero a ottenere l'accesso attraverso credenziali di login. Allo stesso tempo, le VPN collegano più sedi, consentono l'accesso a terzi, supportano dispositivi non gestiti e abilitano la connettività dei dispositivi IoT; tutti questi molteplici casi d'uso fanno sì che questi strumenti vengano impiegati per scopi diversi da quelli per cui sono stati originariamente concepiti, creando spesso lacune nella sicurezza di fronte a minacce sempre più complesse e mutevoli.

Questo report, basato su un'indagine condotta interpellando 382 professionisti di IT ed esperti di cybersecurity, esplora le sfide complesse che colpiscono la sicurezza e l'esperienza utente.Il Report del 2023 sui rischi delle VPN rivela quanto sia complessa oggi la gestione delle VPN e illustra i problemi legati all'esperienza utente, le vulnerabilità ai diversi tipi di attacchi informatici e il loro potenziale di compromettere il profilo di sicurezza generale delle organizzazioni.Prosegue poi esplorando modelli di sicurezza più robusti, e lo zero trust emerge come soluzione valida per proteggere e accelerare la trasformazione digitale.

I PRINCIPALI RISULTATI DELL'INDAGINE INCLUDONO:

Le vulnerabilità delle VPN e l'impatto sulla sicurezza informatica: nonostante il loro ruolo critico, le VPN comportano rischi per la sicurezza: l'88% delle organizzazioni ha espresso una preoccupazione da lieve a estrema riguardo al fatto che le VPN possano mettere a rischio la sicurezza del proprio ambiente. Inoltre, il 45% delle imprese ha confermato di aver subito almeno un attacco che ha sfruttato le vulnerabilità insite in questi strumenti nel corso degli ultimi 12 mesi, mentre 1 su 3 è stata vittima di attacchi ransomware indirizzati alle VPN. La crescente minaccia posta dagli attacchi informatici sottolinea l'urgente necessità di affrontare la sicurezza delle architetture VPN esistenti.

L'utilizzo delle VPN e l'esperienza utente: le VPN vengono impiegate ad ampio spettro, e l'84% degli intervistati identifica l'accesso remoto come principale forma di applicazione. Gli utenti però segnalano un'esperienza scadente: la maggioranza di essi si rivela insoddisfatta della propria esperienza con le VPN (72%), evidenziando la necessità di soluzioni di accesso remoto più semplici e affidabili negli ambienti di lavoro digitalizzati.

Panoramica

Vettori di attacco primari: nell'ultimo anno, un'organizzazione su due ha subito attacchi indirizzati alle VPN. I vettori di attacco diretti alle VPN richiedono un'attenzione particolare, soprattutto per via del loro ruolo critico nel supportare le operazioni aziendali e la comunicazione. Inoltre, gli utenti terzi, come collaboratori e fornitori, rappresentano potenziali backdoor per l'accesso doloso, complicando ulteriormente il lavoro dei team responsabili della sicurezza di rete. Secondo quanto riportato nell'indagine, 9 intervistati su 10 hanno espresso preoccupazione riguardo alla possibilità che utenti terzi possano fungere da potenziali backdoor nella loro rete tramite l'accesso VPN.

Adottare lo zero trust: per la maggior parte delle organizzazioni, la transizione verso un modello zero trust è in cima alla lista delle priorità. Circa 9 intervistati su 10 hanno identificato l'adozione dello zero trust come un'area di interesse, e più di un quarto (27%) sta già implementando questa strategia. Il 37% degli intervistati sta pianificando di sostituire la propria VPN con soluzioni ZTNA (Zero Trust Network Access).

Siamo grati del contributo offerto da Zscaler a questa indagine sul rischio dell'impiego delle VPN. L'esperienza di questa azienda nell'ambito delle soluzioni zero trust e dell'accesso sicuro ha considerevolmente arricchito i nostri risultati.

Siamo certi che gli spunti offerti da questo report consentiranno ai professionisti dell'IT e della sicurezza informatica di poter affrontare al meglio il loro percorso verso la sicurezza zero trust.

Grazie,

Holger Schulze

Holger Schulze
CEO e Fondatore
Cybersecurity Insiders

Cybersecurity
INSIDERS

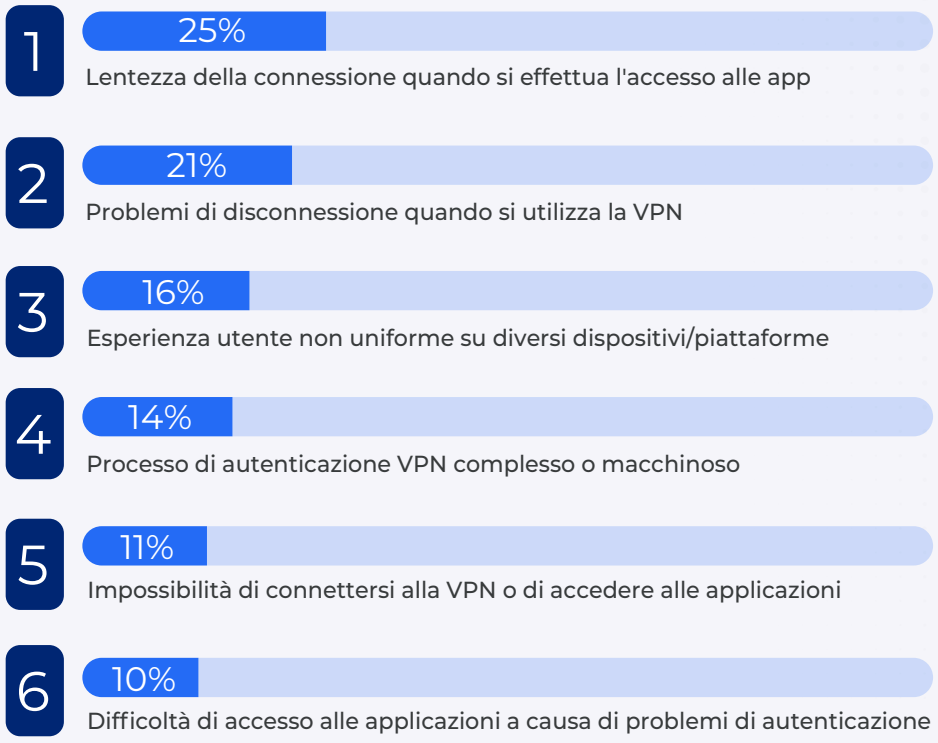
I problemi con la VPN riscontrati dagli utenti finali

Tra le problematiche segnalate, la più frequente è quella relativa alla lentezza della connessione quando si effettua l'accesso alle app tramite VPN, riferita dal 25% degli intervistati. Altri problemi riguardano disconnessioni che si verificano quando si utilizza una VPN (21%) e l'esperienza utente non uniforme su diversi dispositivi e piattaforme (16%).

Alla luce di questi risultati, è evidente che migliorare l'esperienza utente di accesso remoto dovrebbe rappresentare una priorità per molte organizzazioni. Infatti, un'esperienza di accesso fluida e affidabile favorirebbe la produttività, migliorerebbe il livello di sicurezza e supporterebbe la conformità alle policy di sicurezza.

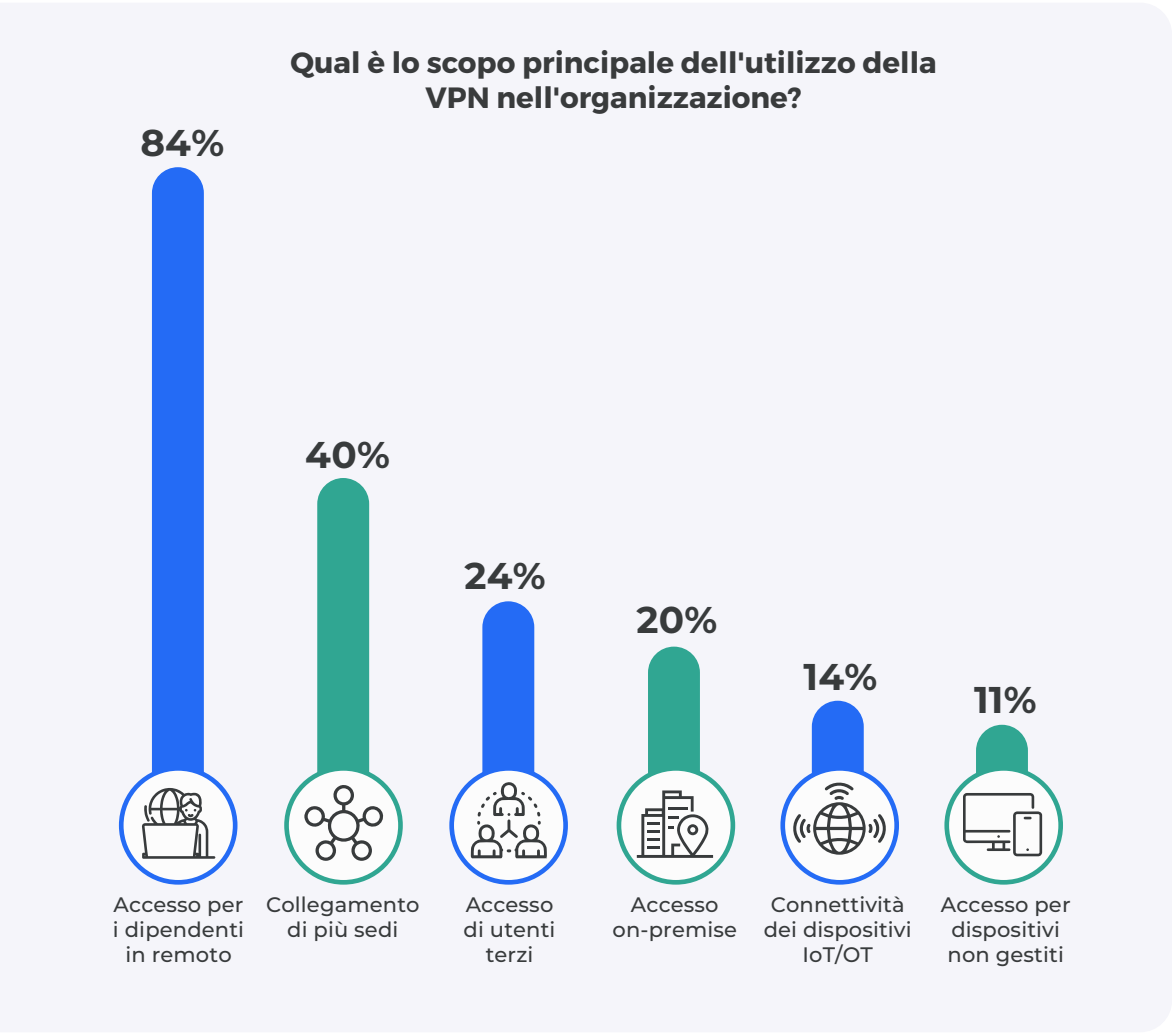
I benefici possono riscontrarsi nell'ottimizzazione delle prestazioni di rete, l'accelerazione della velocità di connessione, la riduzione del numero delle disconnessioni, la semplificazione del processo di autenticazione VPN e l'uniformazione dell'esperienza utente tra le diverse piattaforme. Risulta inoltre fondamentale disporre di meccanismi di supporto consolidati per aiutare gli utenti a risolvere i problemi e le difficoltà che possono verificarsi con l'utilizzo della VPN.

Qual è la lamentela che viene segnalata più frequentemente dagli utenti che accedono alle applicazioni tramite VPN?



Altro 3%

Principale caso d'uso della VPN: l'accesso remoto per i dipendenti



Altro 3%

Le VPN vengono impiegate da moltissimo tempo per collegare i dipendenti in remoto alla rete dell'organizzazione e per un'ampia serie di casi d'uso, come il lavoro da remoto e le connessioni di terze parti.

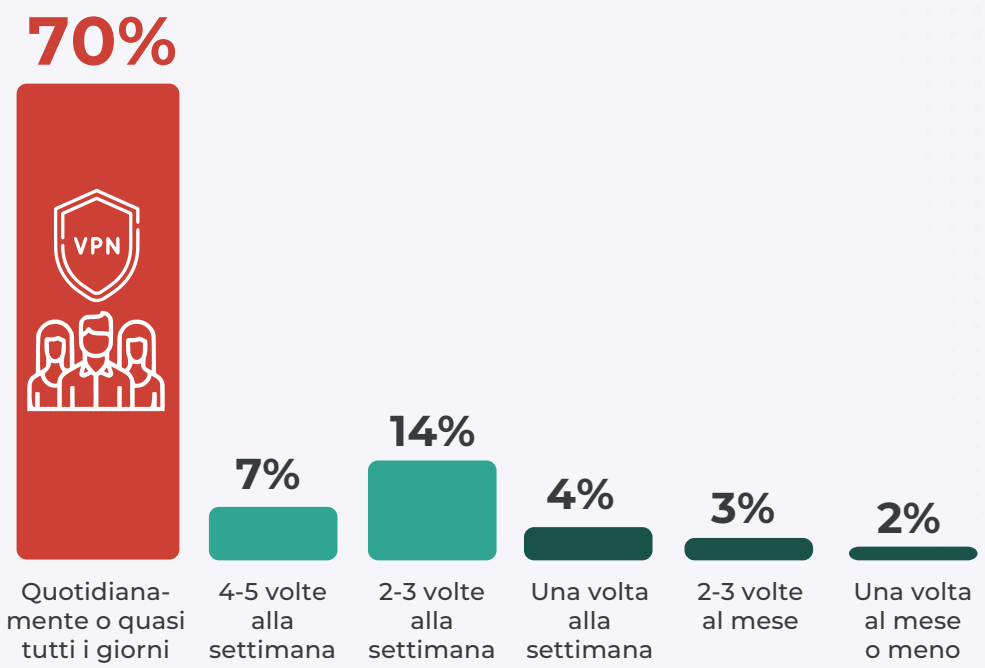
Per la maggior parte delle organizzazioni (l'84%), lo scopo principale dell'utilizzo delle VPN è quello di consentire l'accesso ai dipendenti che lavorano da remoto. Si tratta chiaramente di una conseguenza della nuova tendenza del lavoro a distanza, che nel corso degli ultimi anni ha registrato una crescita significativa.È interessante tuttavia notare che solo l'11% utilizza le VPN per amministrare l'accesso ai dispositivi non gestiti; questo indica che le organizzazioni non stanno pienamente affrontando quella che è una grande vulnerabilità.

Elevata dipendenza dalle VPN

Un numero significativo di utenti finali (il 70%) utilizza le VPN quotidianamente o quasi ogni giorno, dimostrando una forte dipendenza da esse per le operazioni aziendali giornaliere e di routine. Combinando questo dato con quello relativo a coloro che utilizzano le VPN 4-5 volte alla settimana, osserviamo che il 77% di tutti gli intervistati utilizza le VPN per il lavoro praticamente ogni giorno. È interessante notare che nessuno degli intervistati ha dichiarato di utilizzare la VPN meno di una volta al mese, a conferma dell'adozione diffusa di questa tecnologia.

Data l'elevata frequenza di utilizzo, è fondamentale garantire la disponibilità costante e un livello di sicurezza ottimale dei servizi di accesso remoto/VPN.

Con quanta frequenza gli utenti finali dell'organizzazione utilizzano la VPN?



I problemi con l'esperienza utente

Qual è il problema più significativo riscontrato dall'organizzazione con il servizio VPN attualmente in uso?

Limitazioni di scalabilità e flessibilità 11% | Sicurezza e conformità insufficienti 7% | Supporto inadeguato per il lavoro da remoto e la collaborazione 4% | Altro 7%

Le prestazioni e l'esperienza utente relative all'utilizzo dei servizi VPN hanno un impatto significativo sulla produttività dell'organizzazione e sull'efficienza complessiva delle sue operazioni. Una VPN lenta o che si disconnette di frequente può danneggiare considerevolmente l'operatività aziendale e causare frustrazione per gli utenti. Osservando i risultati dell'intervista, il problema più significativo riscontrato con i servizi VPN è l'esperienza utente scadente, per cui il 32% degli intervistati riferisce connessioni lente e disconnessioni frequenti.

Alla luce di questi dati, le organizzazioni dovrebbero dare priorità al miglioramento dell'esperienza utente associata ai propri servizi di accesso remoto, attraverso ad esempio l'aumento della capacità dei server o la scelta di soluzioni per l'accesso sicuro rinomate per la loro velocità e stabilità. È interessante notare che le organizzazioni hanno indicato la sicurezza come un problema relativamente poco importante, nonostante i numerosi attacchi informatici diretti alle VPN registrati nel corso degli ultimi anni.

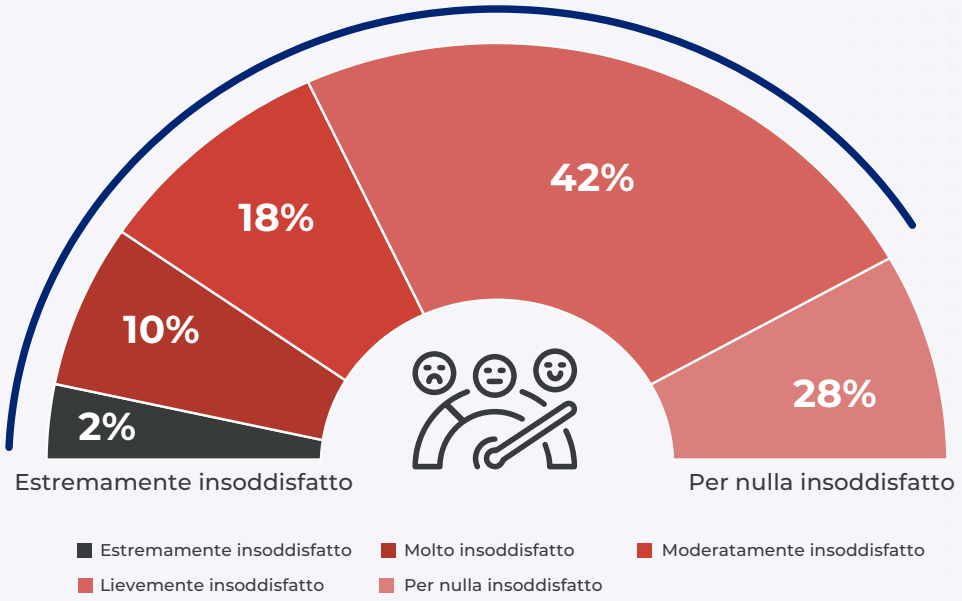
L'insoddisfazione degli utenti verso la VPN

Valutare se l'esperienza degli utenti con la VPN è soddisfacente è fondamentale, in quanto la loro insoddisfazione non solo influisce sulla produttività, ma può portare al mancato rispetto delle policy di sicurezza, pratica che a sua volta potrebbe introdurre vulnerabilità.

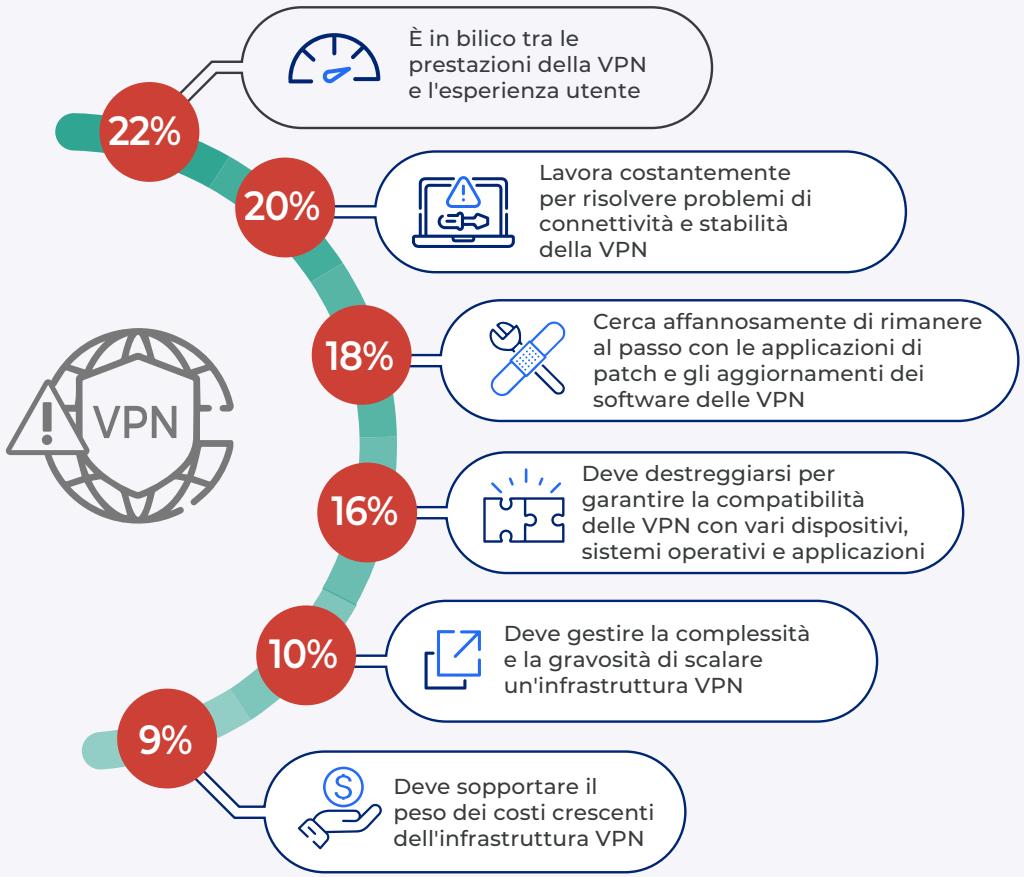
Una maggioranza significativa di utenti (72%) si rivela insoddisfatta della propria esperienza con la VPN, evidenziando la necessità di soluzioni più semplici e affidabili per l'accesso remoto negli ambienti di lavoro digitalizzati.

Quanto sono insoddisfatti gli utenti dell'organizzazione della loro esperienza con la VPN?

72% delle organizzazione è da lievemente a estremamente insoddisfatto dell'esperienza con la VPN



Le problematiche della gestione delle VPN



Altro 5%

L'indagine rivela che il principale problema nella gestione dell'infrastruttura VPN, secondo quanto indicato dal 22% degli intervistati, consiste nell'equilibrio tra le prestazioni della VPN e l'esperienza dell'utente.

Anche la risoluzione dei problemi di connettività e stabilità delle VPN rappresenta una preoccupazione significativa, che riguarda quasi il 20% degli intervistati, seguita subito dopo dall'impegno necessario per rimanere al passo con le frequenti applicazioni di patch e aggiornamenti dei software (18%). È da notare che il 9% degli intervistati cita l'incremento dei costi dell'infrastruttura VPN come problema principale.

I problemi di sicurezza delle VPN

Il livello di sicurezza di una soluzione per l'accesso remoto rappresenta una caratteristica fondamentale per proteggere i dati e i sistemi sensibili dell'organizzazione in modo ottimale. Di fronte a minacce informatiche sempre più avanzate, le VPN possono rafforzare o compromettere il profilo di sicurezza di un'organizzazione, a seconda di come sono state progettate e di come vengono gestite.

Esaminando i risultati dell'indagine emerge che la stragrande maggioranza degli intervistati (88%) teme che la propria VPN possa compromettere la sicurezza dell'ambiente aziendale. Il 22% degli intervistati si dichiara "molto" o "estremamente" preoccupato, a dimostrazione del livello di apprensione nei confronti delle VPN come potenziali punti deboli nella sicurezza.

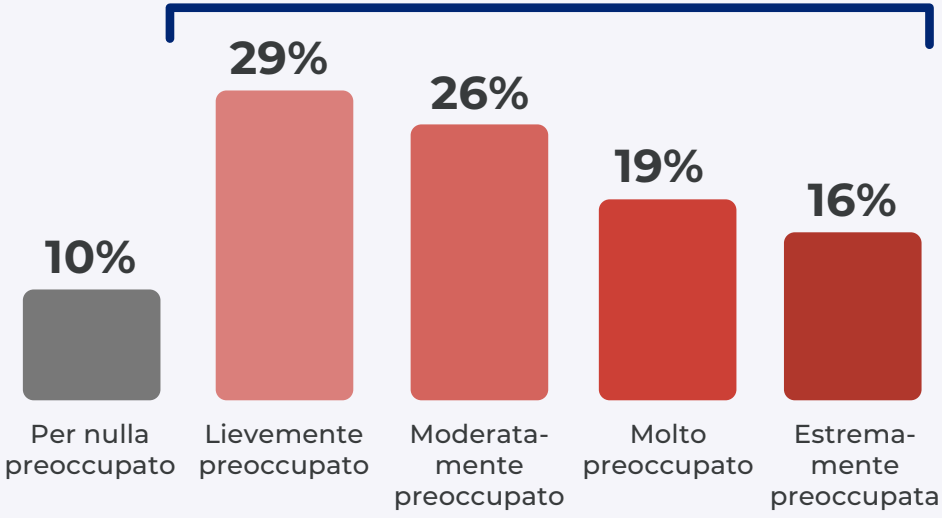
In che misura l'organizzazione è preoccupata del fatto che la VPN possa mettere a rischio la capacità di preservare la sicurezza dell'ambiente?

I problemi di sicurezza relativi a utenti terzi

Qual è il grado di preoccupazione dell'organizzazione riguardo all'eventualità che utenti terzi possano fungere da potenziali backdoor per attacchi alla rete attraverso l'accesso VPN?

Il 90%

degli intervistati teme che gli utenti terzi possano essere causa di potenziali backdoor nella loro rete attraverso l'accesso VPN



Concedere l'accesso a terzi tramite una VPN è una pratica aziendale necessaria, ma solleva anche gravi problemi di sicurezza. Dato che le entità terze potrebbero non aderire a standard di sicurezza informatica altrettanto rigorosi, potrebbero potenzialmente rappresentare backdoor per gli aggressori informatici e la violazione della rete di un'organizzazione.

Nell'indagine, la maggioranza assoluta degli intervistati (90%) ha espresso la preoccupazione che utenti terzi possano fungere da potenziali backdoor nella propria rete attraverso l'accesso VPN. Il 35% degli intervistati totali si è espresso come "molto" o "estremamente" preoccupato; questo suggerisce che l'accesso VPN da parte di utenti terzi desta notevoli preoccupazioni.

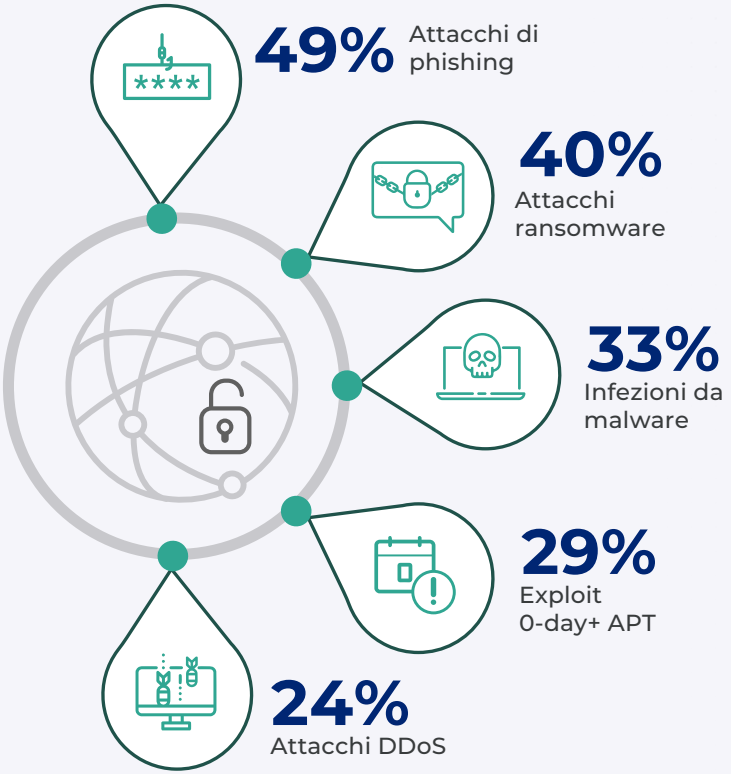
Nel concedere l'accesso a terzi tramite VPN, le organizzazioni devono applicare misure di sicurezza molto rigorose, come la revisione e l'aggiornamento periodico delle autorizzazioni di accesso, l'applicazione di policy che favoriscano l'efficacia delle password e il monitoraggio delle attività di rete alla ricerca di eventuali anomalie. Inoltre, dovrebbero assicurarsi che gli utenti terzi rispettino le proprie policy di sicurezza informatica e prendere in considerazione l'utilizzo di tecnologie avanzate, come l'architettura zero trust, che concede l'accesso solo a chi è autorizzato.

Gli attacchi di phishing costituiscono la metà degli attacchi informatici

Le VPN celano da sempre delle vulnerabilità, e i team IT devono applicare costantemente patch ai propri server VPN. Questo può potenzialmente esporre un'organizzazione a diversi tipi di attacchi informatici, soprattutto perché gli aggressori sono sempre più sofisticati e creativi nelle loro tecniche.

Gli intervistati considerano gli attacchi di phishing (49%) e gli attacchi ransomware (40%) i tipi di attacchi maggiormente in grado di sfruttare le vulnerabilità delle VPN delle loro organizzazioni. Spesso, questi attacchi puntano a ingannare l'utente inducendolo a rivelare informazioni sensibili o a distribuire software dannosi, che bloccano i sistemi fino al pagamento del riscatto.

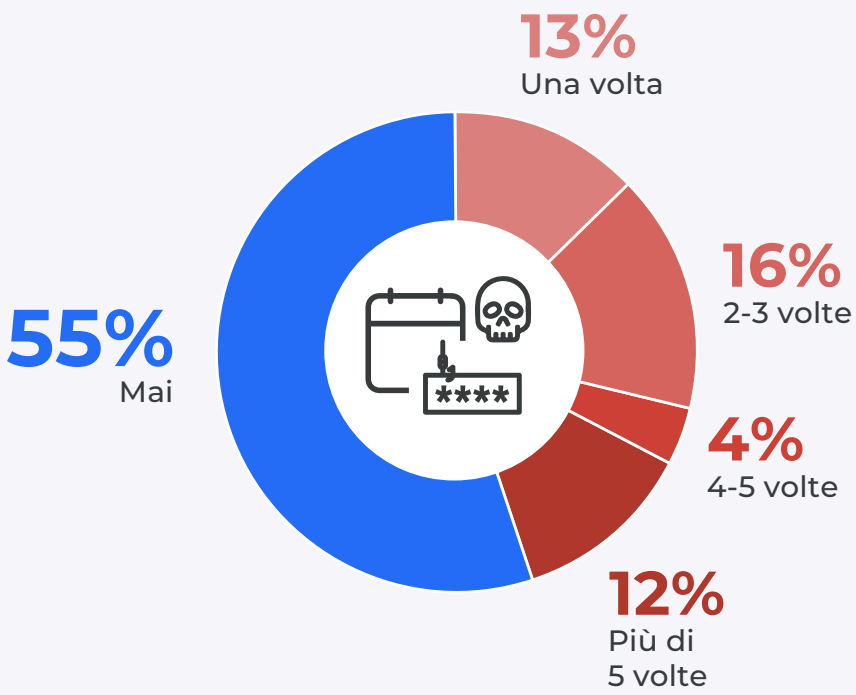
Quali sono i tipi di attacchi informatici maggiormente in grado di sfruttare le vulnerabilità delle VPN dell'organizzazione?



Attacchi man-in-the-middle 22% | Attacchi con escalation dei privilegi 20% | Attacchi con esfiltrazione dei dati 18% | Attacchi di forza bruta 11% | Cross-site scripting 11% | Esecuzione di codice da remoto 9%

Un'organizzazione su due ha subito attacchi diretti alle VPN

Negli ultimi 12 mesi, l'organizzazione ha subito un attacco che ha sfruttato le vulnerabilità di sicurezza presenti nei server VPN?



La sicurezza di un server VPN è fondamentale per preservare l'integrità e la riservatezza dei dati che gestisce. Le organizzazioni dipendono sempre più dalle VPN per supportare il lavoro da remoto, ed eventuali vulnerabilità possono rappresentare bersagli molto interessanti per gli aggressori informatici.

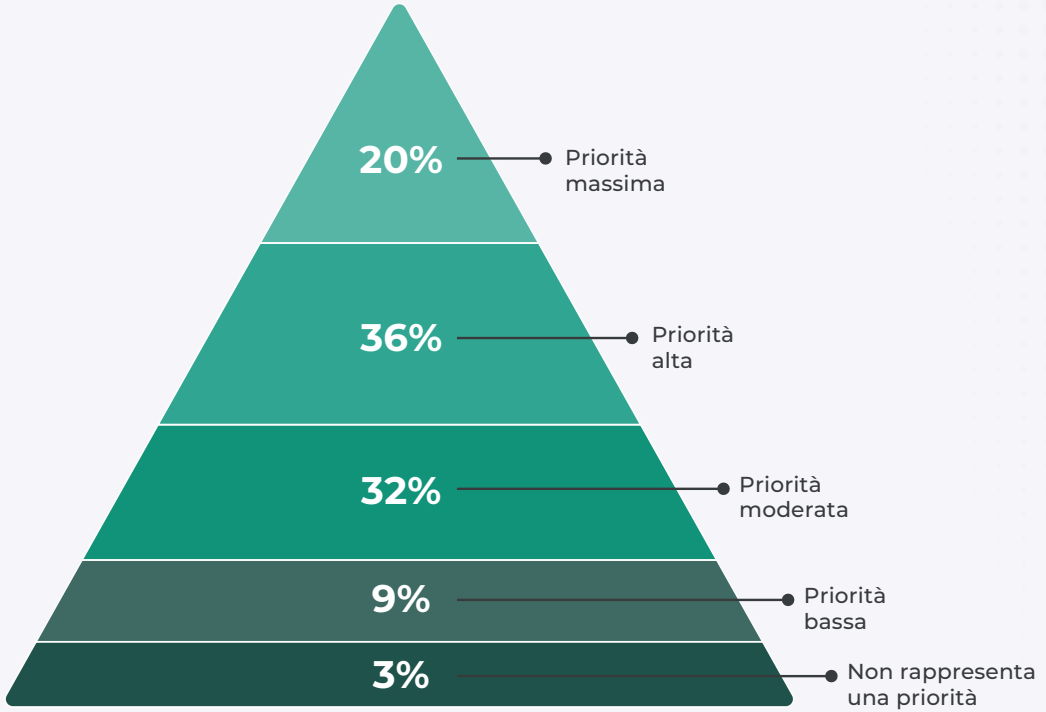
Secondo l'indagine, nel corso degli ultimi 12 mesi una percentuale considerevole di organizzazioni (45%) ha subito uno o più attacchi rivolti ai propri server VPN, i quali hanno sfruttato le vulnerabilità presenti nei software dei server. È dunque evidente l'urgente necessità di adottare soluzioni più sicure per l'accesso remoto.

L'adozione di una strategia zero trust ha la massima priorità

L'adozione dello zero trust, un approccio in cui tutto deve essere verificato, rappresenta una priorità per 9 organizzazioni su 10.

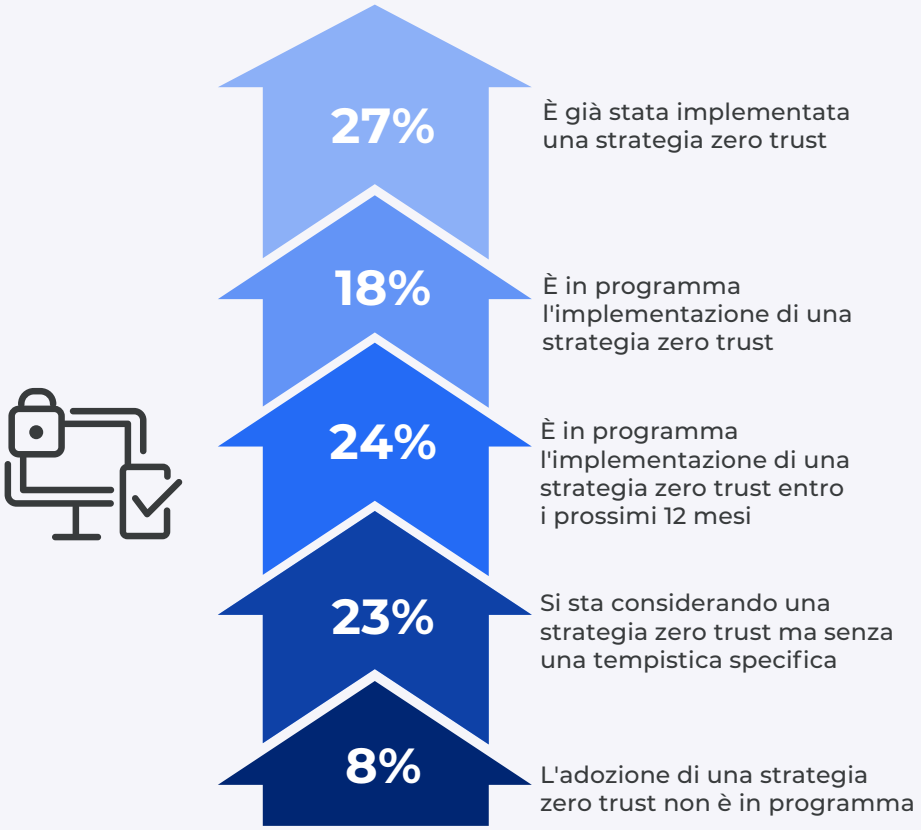
Per sfruttare appieno un'architettura zero trust e rafforzare il profilo di sicurezza, le organizzazioni dovrebbero dare la priorità a metodi di autenticazione a più fattori più rigorosi, verifica continua del traffico, segmentazione della rete, accesso a privilegi minimi e monitoraggio continuo.

Quanto è prioritaria l'adozione di una strategia zero trust per l'organizzazione?



Il focus principale è sull'implementazione dello zero trust

Quali sono i piani dell'organizzazione in merito all'adozione di una strategia zero trust?



Il 92% delle organizzazioni sta già implementando (27%), ha in programma di implementare (42%) o sta prendendo in considerazione una strategia zero trust, a dimostrazione del fatto che le imprese hanno compreso la sua importanza e che questo concetto sta passando dall'essere un termine in voga a rappresentare una realtà concreta per la maggior parte delle aziende.

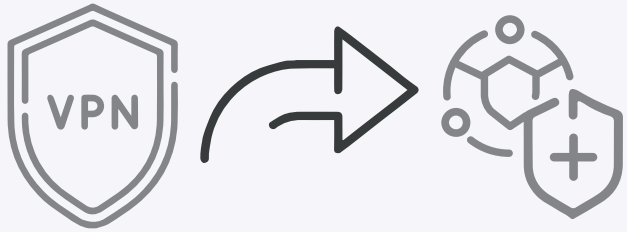
Chi deve ancora definire una tempistica per l'implementazione dovrebbe considerare l'idea di accelerare i propri programmi per preservare la competitività e la sicurezza aziendale. Coloro che non hanno in programma di adottare lo zero trust o che sono ancora incerti rischiano di rimanere indietro nel contrasto a un panorama di minacce informatiche in rapida evoluzione.

I programmi di transizione delle VPN

Il passaggio dalla VPN a soluzioni ZTNA (Zero Trust Network Access) rappresenta una svolta molto significativa nelle moderne strategie di sicurezza informatica, data la maggiore attenzione per l'accesso a privilegi minimi e la microsegmentazione che caratterizzano questo approccio. 4 organizzazioni su 10 stanno passando allo ZTNA; vi è quindi una risposta attiva all'evoluzione degli standard di sicurezza.

Per le organizzazioni che stanno pianificando o considerando una transizione, è fondamentale valutare e scegliere la soluzione ZTNA in grado di soddisfare i requisiti di sicurezza e le esigenze specifiche dell'azienda. Coloro che al momento non hanno in programma di adottare lo ZTNA dovrebbero almeno studiarne i potenziali vantaggi in termini di miglioramento del proprio profilo di sicurezza informatica. Per le aziende che non sono in grado di effettuare una transizione completa, i modelli ibridi possono rappresentare un buon compromesso, in quanto offrono i vantaggi dello ZTNA sfruttando l'infrastruttura VPN esistente.

L'organizzazione ha in programma di sostituire la propria infrastruttura VPN esistente con una soluzione ZTNA (Zero Trust Network Access) nel prossimo futuro?



Il 37%

ha in programma di sostituire la VPN con una soluzione ZTNA nel prossimo futuro

Le best practice da seguire per supportare il percorso verso lo zero trust

Raccomandiamo le seguenti best practice per affrontare con successo il passaggio da un'infrastruttura VPN tradizionale a un'architettura zero trust moderna.

Valutare l'infrastruttura esistente:
inizia con un esame approfondito dell'infrastruttura VPN esistente. Tra gli intervistati, il 32% segnala un'esperienza utente scadente e il 14% mette in evidenza i costi elevati; prima di procedere, è dunque fondamentale comprendere quali sono i problemi specifici da affrontare.

Scegliere la soluzione giusta:
cerca una soluzione zero trust in grado di allinearsi alle esigenze specifiche dell'organizzazione; una soluzione nativa del cloud e definita da software può contribuire a semplificare la gestione, ridurre i costi e migliorare l'esperienza utente, problemi comunemente associati alle VPN.

Implementare l'accesso a privilegi minimi:
una caratteristica basilare dello zero trust è che l'utente deve poter accedere solo alle specifiche risorse necessarie per svolgere il proprio ruolo.

Pianificare l'adattamento delle prestazioni:
opta per una soluzione scalabile e in grado di adattarsi alla crescita dell'azienda. La nostra indagine ha indicato che circa l'11% delle organizzazioni riscontra problemi di scalabilità con le proprie VPN. Una soluzione con base cloud, al contrario, è in grado di gestire efficacemente questo tipo di esigenza.

Rivedere e aggiornare regolarmente le proprie policy di sicurezza:
rivedi e aggiorna regolarmente le policy di sicurezza, in quanto ciò aiuta a preservare la solidità del profilo di sicurezza.

Abilitare l'accesso sicuro per tutti gli utenti:
adotta una soluzione in grado di fornire un accesso sicuro ai dipendenti in remoto, alle terze parti e ai dispositivi non gestiti, prediligendo le piattaforme che supportano qualsiasi utente, ovunque e su qualsiasi dispositivo.

Monitoraggio e miglioramento continui:
adotta una strategia di monitoraggio continuo per identificare e rispondere ai potenziali problemi prima che si aggravino. Il rilevamento e la risposta proattivi sono infatti la chiave per un'implementazione efficace dello zero trust.

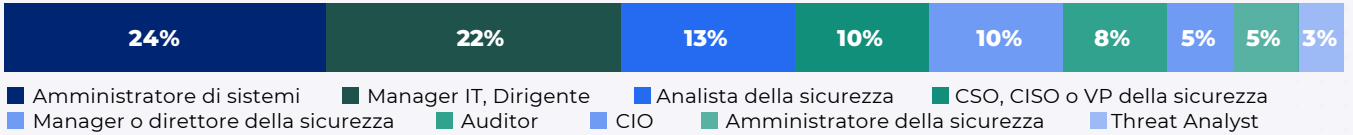
Metodologia e dati demografici

Questo report si basa sui risultati di un'approfondita indagine online a cui hanno partecipato 382 professionisti IT e di sicurezza informatica svolta a giugno del 2023. L'indagine è stata condotta con lo scopo di identificare le ultime tendenze nelle soluzioni adottate dalle aziende, le sfide, le lacune e le soluzioni preferite in relazione ai rischi delle VPN. Gli intervistati vanno da dirigenti tecnici a professionisti della sicurezza IT, e rappresentano in modo bilanciato organizzazioni di varie dimensioni operanti in più settori.

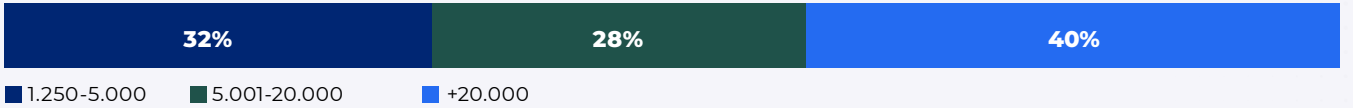
Livello carriera

Reparto

Ruolo primario



Dimensioni dell'azienda



Settore

Informazioni su 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 dagli attacchi informatici e dalla perdita di dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la più grande piattaforma di sicurezza cloud inline del mondo.

Per saperne di più, visita zscaler.it o seguici su Twitter @zscaler.

zscaler.it

Cybersecurity
INSIDERS

Cybersecurity Insiders riunisce oltre 600.000 professionisti della sicurezza informatica e fornitori di tecnologia di alto livello per facilitare la risoluzione intelligente dei problemi e la collaborazione nell'affrontare le attuali sfide più critiche di cybersecurity.

Il nostro approccio si concentra sulla creazione e la cura di contenuti esclusivi, volti a istruire e formare i professionisti della cybersecurity sulle ultime tendenze, soluzioni e best practice da seguire. Con studi di ricerca approfonditi, recensioni imparziali dei prodotti, guide pratiche, webinar coinvolgenti e articoli formativi, ci impegniamo a fornire risorse che rispondano in modo concreto alle complesse sfide esistenti nel panorama della sicurezza informatica.

Contattaci oggi stesso per scoprire come Cybersecurity Insiders può aiutarti a emergere in un mercato altamente competitivo e ad accrescere la domanda, la visibilità e la presenza del marchio a livello di leadership di pensiero.

Inviaci un'e-mail a **info@cybersecurity-insiders.com** oppure visita **cybersecurity-insiders.com**