Abbattere le barriere: La strategia di CIO e CISO per supportare la nuova forza lavoro flessibile

Questo approfondito report di ricerca illustra le tecniche più efficaci per passare da un'infrastruttura legacy esposta a una strategia zero trust efficiente.

UN REPORT DI RICERCA DI HMG STRATEGY SUPPORTATO DA ZSCALER

HMG STRATEGY

zscaler™

RIEPILOGO

Mentre entriamo in una nuova fase della pandemia globale, molte aziende sono alle prese con il problema di come riuscire a far rientrare i propri dipendenti in ufficio dopo oltre due anni di assenza. Diverse indagini dimostrano che sempre più persone desiderano lavorare in modo flessibile, con un mix tra il lavoro in sede e a distanza, e se non vi è la libertà di decidere quando e dove lavorare, molti scelgono di abbandonare le aziende alla ricerca di nuove opportunità.

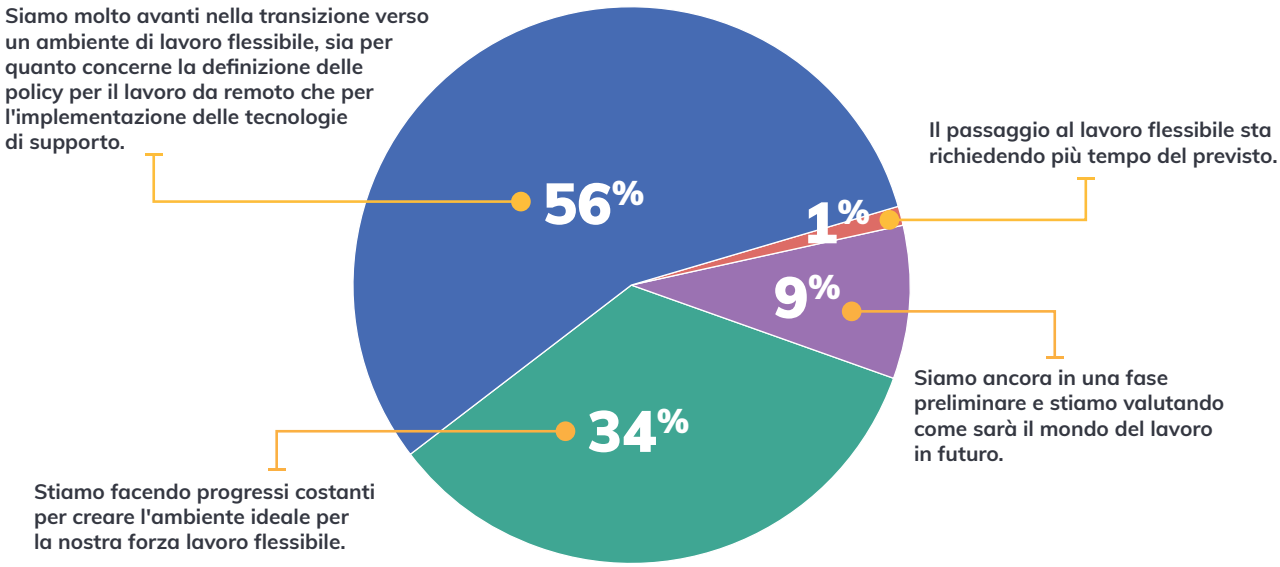
Ma come si fa a trasformare con successo il business per supportare al meglio il futuro del lavoro flessibile? E come possono CIO e CISO allineare il loro lavoro a quello degli altri membri della C-suite per offrire un ambiente di lavoro agile e produttivo, proteggendo al contempo l'azienda?

Una recente indagine condotta da HMG Strategy su 138 CIO, CISO e leader delle tecnologie aziendali sponsorizzata da Zscaler rivela che: se da un lato il 56% degli intervistati dichiara che le proprie organizzazioni sono "molto avanti" nella transizione verso un ambiente di lavoro flessibile, sia per quanto concerne la definizione di policy per il lavoro da remoto, che per l'implementazione delle tecnologie di supporto, quasi la metà (44%) dei dirigenti ritiene questa transizione un'operazione ancora in corso.

In realtà, in questo 44%, quasi una persona intervistata su cinque afferma che la transizione verso un ambiente di lavoro flessibile è ancora in fase preliminare, e che l'azienda sta ancora valutando come sarà il mondo del lavoro in futuro.

Adattarsi al mondo del lavoro flessibile

Come definirebbe la transizione della sua organizzazione dal lavoro da remoto al lavoro flessibile?



Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

"La maggior parte delle organizzazioni riesce a supportare la transizione dal lavoro da remoto a quello flessibile, ma in modo limitato", dichiara **Bryan Green**, CISO di Zscaler per le Americhe. Ad esempio, dall'inizio della pandemia, gran parte delle aziende ha effettuato investimenti temporanei e a breve termine per espandere l'uso di tecnologie VPN o bypassare le applicazioni sensibili ad alta larghezza di banda, come i sistemi di videoconferenza, per affrontare il passaggio al lavoro da remoto. "Ma non è detto che a lungo termine queste siano le decisioni giuste, in termini di sicurezza", aggiunge Green.

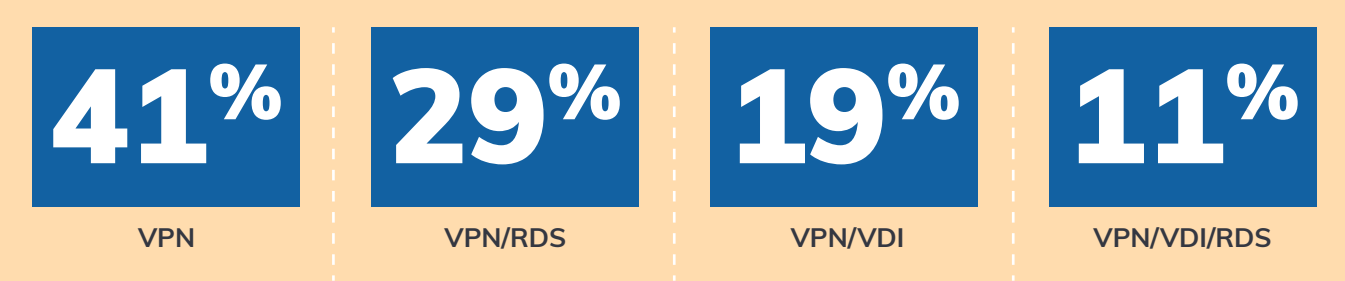
Avendo agito da "promotori del cambiamento" durante la pandemia, i responsabili della tecnologia si trovano in una posizione ideale per aiutare le loro organizzazioni ad affrontare la prossima fase dell'evoluzione degli ambienti di lavoro, assicurando l'implementazione delle tecnologie giuste per soddisfare le esigenze dei lavoratori flessibili e creando un ambiente agile, produttivo e sicuro, sia per i lavoratori in ufficio che per quelli da remoto. Tuttavia, come indica questa ricerca, è necessario un ulteriore sforzo per far sì che questo concetto diventi la nuova realtà.

HMG Strategy ha collaborato con Zscaler per comprendere più a fondo le sfide e le opportunità che le aziende si trovano di fronte durante la transizione verso un ambiente di lavoro flessibile e sicuro, compresi gli ostacoli tecnologici e culturali che impediscono di raggiungere questo obiettivo. Questo report di ricerca illustra:

- Le difficoltà tecniche nell'ottenere un ambiente di lavoro sicuro e flessibile, comprese le problematiche delle infrastrutture legacy, come le tecnologie VPN.
- I rischi che le organizzazioni devono affrontare per garantire l'accesso alle applicazioni a una forza lavoro flessibile.
- Le sfide per la sicurezza associate al fornire l'accesso alle applicazioni private a lavoratori che operano sia da remoto che dall'ufficio.
- Un'architettura solida come soluzione alle insidie per la sicurezza generate dall'ambiente di lavoro flessibile, supportata dallo zero trust.

Gli strumenti per consentire l'accesso alle applicazioni

Quali sono le tecnologie per l'accesso alle applicazioni attualmente in uso nella sua organizzazione?



Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

"La maggior parte delle organizzazioni riesce a supportare la transizione dal lavoro da remoto a quello flessibile, ma in modo limitato".

BRYAN GREEN
CISO, Americhe
Zscaler

Superare le barriere per ottenere un ambiente di lavoro agile, sicuro e flessibile

Sebbene negli ultimi anni le aziende abbiano continuato ad adottare software come servizio (SaaS) e servizi di cloud pubblico, molte organizzazioni si trovano ancora nella fase di migrazione verso il cloud. Secondo uno studio di Foundry, nel corso del prossimo anno, il 63% delle aziende prevede di spostare la maggior parte o la totalità della propria infrastruttura IT sul cloud, una percentuale che attualmente è pari al 41%.

Sebbene l'adozione del cloud stia accelerando, le aziende continuano a investire massicciamente in data center e infrastrutture on-premise.

"Nonostante siano passati 16 anni da quando AWS ha iniziato a lanciare infrastrutture cloud pubbliche e private, è solo da due anni, con la pandemia di COVID, che la spinta verso il lavoro da remoto ha cominciato concretamente ad accelerare", afferma Green, "e sono molte le aziende che si trovano ad affrontare le sfide derivanti dalle complessità relative a persone, processi e tecnologie nelle loro organizzazioni".

Un'altra questione complessa associata al passaggio al lavoro flessibile è quella delle dinamiche di leadership. Visti gli enormi investimenti immobiliari delle aziende in uffici di proprietà o in affitto, molti dirigenti vogliono assicurarsi che gli spazi siano utilizzati in modo efficiente. In alcuni casi, la dirigenza senior impone ai dipendenti di lavorare due o tre giorni alla settimana in un ufficio dedicato, ma sono molti i lavoratori che si oppongono a queste direttive.

Secondo una ricerca di Kastle Systems, una società di sicurezza gestita che traccia gli ingressi negli edifici adibiti a uffici aziendali, nella prima settimana successiva al Labor Day del 2022, la festa del lavoro statunitense, l'utilizzo degli uffici in dieci grandi aree metropolitane degli Stati Uniti è stato quasi pari al 50% delle presenze registrate nel 2020, prima della pandemia. Ancora oggi, l'affluenza in ufficio è bassa se rapportata al periodo precedente alla pandemia, anche se diversi studi hanno evidenziato un aumento negli ultimi mesi.

"Il management di molte organizzazioni si trova ad affrontare la realtà di avere questi enormi investimenti in immobili da gestire", dichiara Green. "E vuole che le persone siano sul posto per collaborare, ma questa è una sfida molto complessa".

Affrontare le sfide della sicurezza informatica

Quando a marzo del 2020 le aziende sono passate al lavoro da remoto, si sono rese evidenti molteplici lacune nel loro approccio al monitoraggio e alla tutela della forza lavoro a distanza. Per cominciare, molte organizzazioni si sono affidate alle reti private virtuali (VPN) per consentire ai dipendenti di inviare e ricevere dati attraverso reti condivise o pubbliche. Ciò ha messo in luce diverse vulnerabilità delle VPN:

- Ogni gateway VPN ha un listener in entrata che lo rende una superficie di attacco esposta.
- Il gateway VPN diventa quindi un punto di attracco che viene sfruttato dagli hacker per lanciare altri attacchi più sofisticati.
- La VPN è aperta per natura, e questo costringe i team di sicurezza a bloccare esplicitamente i dipendenti negando loro l'accesso alle applicazioni e ai sistemi se non sono o non dovrebbero essere autorizzati ad accedervi.

Modernizzazione dell'ambiente di lavoro flessibile

Molti ostacoli all'ottenimento di un ambiente di lavoro flessibile, agile e sicuro sono legati alle infrastrutture obsolete e alla mancanza degli strumenti necessari per prevenire la perdita di dati e l'accesso non autorizzato alle applicazioni.

Le principali barriere all'ottenimento di un ambiente di lavoro agile, sicuro e flessibile

30%

Anche se consentiamo attivamente l'uso dei dispositivi personali (BYOD), non disponiamo degli strumenti necessari per ridurre al minimo il rischio legato alla perdita di dati e all'accesso non autorizzato alle risorse interne.

20%

La nostra infrastruttura VPN rallenta sensibilmente la connettività a Internet e influisce negativamente sulla produttività dei dipendenti.

22%

Il nostro business si avvale di collaboratori e partner terzi, ma fornire loro un accesso sicuro alle applicazioni interne è una vera e propria sfida.

16%

La latenza della nostra rete VDI è frustrante per i dipendenti e rende impossibili anche le attività più semplici sui desktop virtuali.

7%

Anche se consentiamo attivamente l'uso dei dispositivi personali (BYOD), non disponiamo degli strumenti necessari per ridurre al minimo il rischio legato alla perdita di dati e all'accesso non autorizzato alle risorse interne. Il nostro business si avvale di collaboratori e partner terzi, ma fornire loro un accesso sicuro alle applicazioni interne è una vera e propria sfida.

5%

La latenza della nostra rete VDI è frustrante per i dipendenti e rende impossibili anche le attività più semplici sui desktop virtuali. Il nostro business si avvale di collaboratori e partner terzi, ma fornire loro un accesso sicuro alle applicazioni interne è una vera e propria sfida.

Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

"Se si dispone di una combinazione di VPN per l'accesso remoto e VPN site-to-site, ci si ritrova con un'enorme superficie di attacco che potenzialmente consente a utenti o attori malintenzionati di sopraffare l'infrastruttura aziendale".

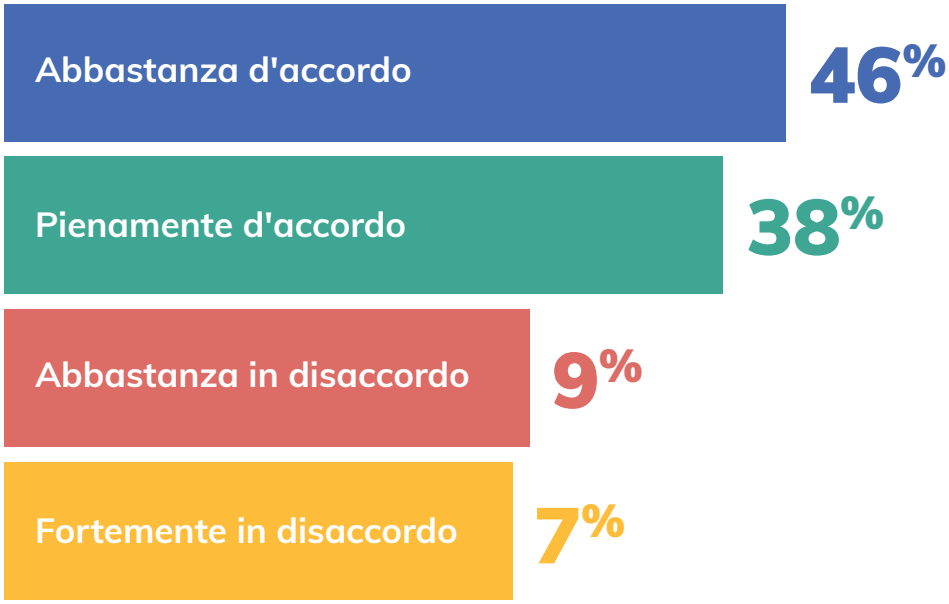
BRYAN GREEN
CISO, Americhe
Zscaler

"Quando si crea una connessione VPN, si estende di fatto la rete aziendale a varie sedi", afferma Green, che ha iniziato a lavorare sui concentratori VPN di Cisco nel 2003. "Se si dispone di una combinazione di VPN per l'accesso remoto e VPN site-to-site, ci si ritrova con un'enorme superficie di attacco che potenzialmente consente a utenti o attori malintenzionati di sopraffare l'infrastruttura aziendale. A meno che non si siano adottati determinati tipi di firewall o di segmentazione, gli aggressori potranno accedere all'infrastruttura senza problemi".

Calo della produttività

L'uso dell'accesso remoto e delle VPN site-to-site non solo estende in modo esponenziale la superficie di attacco di un'organizzazione, ma riduce anche la produttività dei dipendenti che lavorano in modalità flessibile.

Indichi in che misura è d'accordo con la seguente affermazione: la lentezza delle prestazioni della VPN influisce negativamente sulla produttività dei dipendenti che lavorano in modalità flessibile.



Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

Le vulnerabilità intrinseche nell'uso delle VPN sono solo alcuni dei motivi per cui le organizzazioni dovrebbero passare a un'architettura zero trust per tutelare il proprio ambiente di lavoro flessibile. Oltre a impedire che le organizzazioni subiscano violazioni costose, un'architettura zero trust offre una riduzione della complessità, una protezione dei dati di livello superiore e un'esperienza migliore per i dipendenti, eliminando al contempo la superficie di attacco.

Nelle prossime sezioni di questo report, esploreremo le sfide per la sicurezza associate all'accesso a privilegi eccessivi e i vantaggi operativi e aziendali derivanti dall'adozione di una strategia zero trust.

Eliminare l'accesso a privilegi eccessivi per supportare un ambiente flessibile e sicuro

Anche se in molte organizzazioni alcune categorie di dipendenti lavorano in remoto già da anni, il passaggio generalizzato al digitale avvenuto a marzo del 2020 ha ampliato in modo esponenziale il loro livello di digitalizzazione e, conseguentemente, la loro superficie di attacco.

L'adozione sempre più diffusa di cloud pubblici da parte delle imprese aumenta anche il rischio di fornire un accesso a privilegi eccessivi e di esporre i dati critici.

L'esposizione ai rischi della forza lavoro flessibile

Se utilizzate in un ambiente di lavoro flessibile, le infrastrutture legacy creano molteplici forme di esposizione che i team di sicurezza si trovano a dover affrontare, tra cui l'accesso alle applicazioni a privilegi eccessivi per dipendenti, collaboratori e utenti compromessi che accedono alle risorse di rete.

Quali rischi sta affrontando la sua organizzazione per garantire l'accesso alle applicazioni a una forza lavoro flessibile?

31%

Accesso a privilegi eccessivi per i dipendenti o i fornitori terzi.

26%

Utenti compromessi che accedono alle risorse di rete.

18%

Perdita di dati accidentale e/o dolosa.

15%

Dispositivi ad alto rischio che accedono alle risorse di rete (come dispositivi sconosciuti e non conformi

10%

Attacchi alle applicazioni (come attacchi DoS, cross-site scripting, injection).

Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

"L'accesso a privilegi eccessivi è un problema di sicurezza molto grave che dobbiamo affrontare e che abbiamo faticato a risolvere nel settore", dichiara Green, facendo un'analogia con le interazioni dei clienti in una filiale bancaria. In una filiale di una banca, il cliente non fornisce a ogni cassiere o dipendente la chiave della propria cassetta di sicurezza. Ma fornire a dipendenti e utenti l'accesso logico a diversi tipi di applicazioni in base al ruolo "è molto più impegnativo da implementare rispetto all'accesso fisico", afferma Green.

Fortunatamente gli strumenti moderni, come quelli per la gestione dei diritti dell'infrastruttura cloud (CIEM), consentono di gestire i rischi associati all'accesso a privilegi eccessivi fornendo una visibilità avanzata sui diritti e sui rischi dell'accesso sul cloud, e consentono alle organizzazioni di adottare una strategia che riduca al minimo i privilegi.

Nella sezione finale di questo report di ricerca condivideremo i fattori che stanno portando i responsabili della sicurezza e della tecnologia ad adottare strategie di sicurezza zero trust, insieme ai vantaggi operativi e commerciali derivanti dall'applicazione di questo modello.

Mancanza di fiducia negli strumenti di sicurezza esistenti

Solo un terzo dei responsabili della sicurezza e della tecnologia ha espresso una forte fiducia nella capacità degli strumenti di sicurezza adottati dalla propria organizzazione di identificare un utente compromesso o una minaccia interna che accede alle risorse di rete.

Quanta fiducia ripone nel fatto che gli strumenti di sicurezza esistenti siano in grado di identificare un utente compromesso o una minaccia interna che accede alle risorse di rete?

34%

Molta fiducia

62%

Moderata fiducia

4%

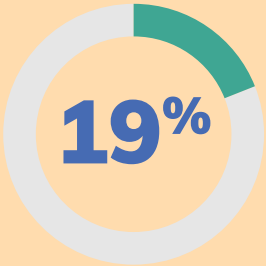
Nessuna fiducia

Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

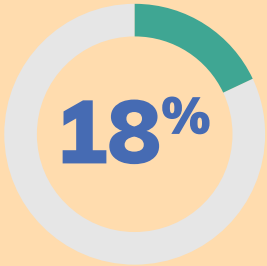
Le lacune nella sicurezza dell'accesso alle applicazioni private

Non sono solo le applicazioni pubbliche a essere esposte a vulnerabilità nella sicurezza; anche le applicazioni private, rese disponibili attraverso i gateway Internet, possono essere vulnerabili agli attacchi.

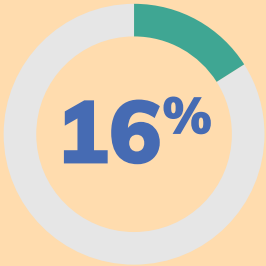
Quali dei seguenti scenari ha incontrato la sua organizzazione nel fornire l'accesso alle applicazioni private ai lavoratori in remoto e in ufficio?



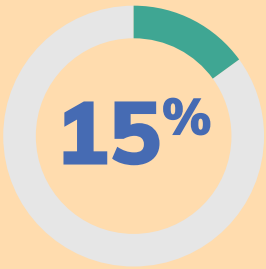
Gli utenti si sentono frustrati a causa di policy di accesso incoerenti e problemi di connettività.



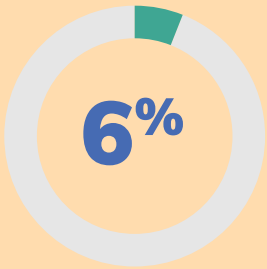
Per fornire l'accesso, le applicazioni private sono esposte a Internet, e questo le rende vulnerabili agli attacchi.



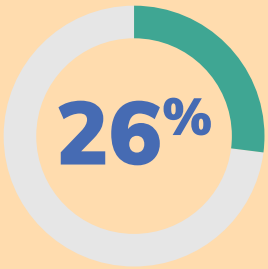
I dipendenti e gli utenti terzi hanno pieno accesso alla rete aziendale, e questo incrementa il rischio di subire movimento laterale.



Per consentire al personale di accedere alle applicazioni private, effettuiamo il backhauling degli utenti in remoto verso i nostri data center, rallentando così la loro connessione a Internet.



Per consentire al personale di accedere alle applicazioni private, reindirizziamo gli utenti dell'ufficio o delle filiali verso il nostro data center, danneggiando così le prestazioni.



Non abbiamo riscontrato nessuno di questi scenari.

Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

Il viaggio verso una strategia zero trust

Con l'aumento dei problemi di sicurezza associati ai dispositivi personali non gestiti impiegati negli uffici domestici, il continuo ricorso alle VPN ha esposto molte organizzazioni a dei rischi. Se a questo si aggiungono le vulnerabilità associate a un accesso a privilegi eccessivi alle applicazioni, risulta evidente che l'infrastruttura legacy adottata da molte aziende per supportare la forza lavoro flessibile non solo è inefficiente, ma è del tutto insostenibile.

Questi sono solo alcuni dei motivi per cui la maggior parte dei CISO e dei responsabili della sicurezza aziendale sta adottando delle architetture zero trust moderne per rafforzare le proprie difese e tutelare integralmente le organizzazioni.

"Innanzitutto, una soluzione ZTNA migliora i risultati per la sicurezza, perché riduce la superficie di attacco", dichiara Green. "Inoltre, lo ZTNA migliora notevolmente l'esperienza utente e le prestazioni".

Con il lavoro flessibile che è sempre più diffuso, i responsabili C-Level della tecnologia stanno valutando molto seriamente le alternative all'architettura legacy. Il rafforzamento della sicurezza e l'aumento della produttività sono stati i fattori che hanno indotto la maggior parte delle organizzazioni ad adottare lo ZTNA. Tutte le imprese che hanno adottato l'approccio zero trust hanno registrato una significativa riduzione dei costi e della complessità, che ha consentito loro di concentrarsi molto di più sul business.

Le motivazioni alla base dell'adozione dello zero trust

Oltre il 35% degli intervistati sta prendendo in considerazione di adottare lo zero trust invece delle soluzioni legacy per proteggere le proprie soluzioni tecnologiche e i dipendenti nel loro ambiente di lavoro flessibile.

Cosa ha indotto la sua organizzazione ad adottare una strategia di sicurezza zero trust?

29%

Stiamo valutando la possibilità di passare alla sicurezza zero trust, ma non abbiamo ancora preso una decisione.

Ci siamo resi conto che i firewall e le VPN tradizionali sono più facilmente aggirabili dagli aggressori e consentono di muoversi lateralmente senza limitazioni. **21%**

Siamo passati a una strategia zero trust per offrire una connettività agile, sicura e flessibile alla forza lavoro. **20%**

Ci siamo resi conto che i firewall e le VPN tradizionali avevano generato una superficie di attacco molto estesa. **15%**

Al momento non abbiamo intenzione di adottare una strategia di sicurezza zero trust. **15%**

Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

"Supponiamo che un utente malintenzionato riesca a stabilire un punto di ingresso o a compromettere un'infrastruttura all'interno dell'ambiente aziendale. Dal punto di vista della kill chain, è necessario assicurarsi che l'hacker non possa continuare a muoversi lateralmente all'interno dell'organizzazione", afferma Green. "Ma soprattutto, che non sia in grado di esfiltrare i dati dall'ambiente e di rubare quindi proprietà intellettuale riservata, segreti commerciali o dati dei clienti. Credo che la combinazione di questi tre elementi sia davvero una delle ragioni più importanti per orientarsi verso una soluzione basata sull'accesso zero trust".

Una strategia zero trust offre anche ulteriori vantaggi, soprattutto in un mercato del lavoro ristretto. **L'84%** dei responsabili della tecnologia che hanno preso parte alla ricerca di HMG Strategy ritiene che l'adozione di un modello di lavoro agile, flessibile e sicuro abbia contribuito alla capacità della loro organizzazione di attrarre e trattenere nuovi professionisti.

"Credo che l'alta percentuale dei dirigenti che vedono questa connessione rifletta la flessibilità e la libertà con cui i dipendenti scelgono di lavorare", continua Green.

Il 55% dei partecipanti alla ricerca condotta da HMG Strategy indica che il passaggio al lavoro flessibile ha portato le organizzazioni a rivalutare la loro infrastruttura di accesso remoto legacy.

Nel frattempo, se da un lato molti team dirigenziali si concentrano sui costi, la transizione da controlli legacy antiquati e costosi a una moderna infrastruttura zero trust consente alle aziende di reagire alle mutevoli condizioni di mercato in modo rapido e flessibile, riducendo al contempo i costi e i rischi per l'impresa.

Sostituendo un insieme incoerente di strumenti legacy con un'architettura zero trust, è inoltre possibile consentire ai team di sicurezza di semplificare e gestire in modo più efficace i controlli di sicurezza a livello generale. "Il passaggio a un modello zero trust permette di applicare un numero ridotto di controlli di sicurezza e di utilizzare un'unica console per implementarli", osserva Green.

Dopo il passaggio all'ambiente di lavoro digitale a marzo del 2020, i dipendenti hanno dimostrato non solo quanto possano essere produttivi anche lavorando da remoto, ma anche quanto desiderino maggiore flessibilità nella loro vita personale e professionale. È sempre più evidente: il modello di lavoro tradizionale, che prevede che i dipendenti siano in ufficio tutto il giorno, appartiene ormai al passato. Va ribadito però che le tecnologie legacy, come le VPN, non offrono l'agilità o la protezione necessaria per tutelare i dati sensibili in un ambiente di lavoro flessibile. È necessario un approccio nuovo e più efficace.

"Per le organizzazioni, lo zero trust rappresenta una fantastica opportunità per migliorare il modo di operare in un ambiente di lavoro flessibile" afferma Green.

Le tecnologie zero trust che proteggono il lavoro flessibile

Quali delle seguenti tecnologie zero trust sta utilizzando la sua organizzazione per supportare il lavoro flessibile e sicuro?

19%
Autenticazione a più fattori

16%
Sicurezza degli endpoint

14%
Firewall cloud

10%
Prevenzione della perdita dei dati

9%
Secure Web Gateway

32%
Altro

Fonte: sondaggio Secure Hybrid Workplace 2022, condotto da HMG Strategy nel secondo e terzo trimestre del 2022 su 138 CIO, CISO e responsabili della tecnologia.

Informazioni su HMG Strategy

HMG Strategy è una piattaforma digitale rinomata globalmente che aiuta i responsabili della tecnologia a rivoluzionare l'impresa e rimodellare il mondo del business. La rete globale di HMG Strategy è composta da oltre 400.000 CIO, CTO, CISO, CDO, responsabili delle tecnologie aziendali, dirigenti del settore della ricerca, investitori in venture capital, esperti del settore e leader di pensiero di alto livello.

Informazioni su Zscaler

Zscaler 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 dei 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 sull'SSE, è la più grande piattaforma di cloud security inline del mondo.