White paper

Affrontare le cinque principali sfide della sicurezza di rete con lo zero trust

Negli ultimi decenni, le reti hub and spoke hanno esteso la rete aziendale agli utenti e alle sedi in remoto, compresi gli uffici delle filiali. Questa tipologia di rete era stata concepita e ottimizzata per il collegamento a un data center centralizzato, dove venivano applicati i controlli di sicurezza. Dato che all'epoca tutto faceva parte di una rete piatta, la sicurezza doveva creare una barriera tra la rete attendibile e il mondo esterno (Internet). Questo modello di sicurezza perimetrale, che impiegava i firewall, era noto come modello a castello e fossato, e funzionava bene in passato, quando tutti gli utenti e le applicazioni erano locali. Tuttavia, le esigenze aziendali sono cambiate con l'aumento esponenziale del lavoro da remoto e il passaggio sul cloud di un numero crescente di applicazioni.

Questi cambiamenti hanno generato nuove difficoltà per le organizzazioni che applicano le architetture di sicurezza della rete alla protezione della forza lavoro ibrida e delle applicazioni cloud. Nelle prossime pagine le descriveremo nel dettaglio.

N°1

Rischi sconosciuti e non controllati che provocano interruzioni delle operazioni e perdite

La sicurezza informatica diventa più complessa ogni giorno a causa delle minacce avanzate e degli attacchi gestiti da aggressori sofisticati, in grado di individuare e violare firewall, VPN e firewall virtuali cloud. Ogni firewall che si interfaccia con Internet, sia nel data center che nel cloud o nella filiale, può essere individuato, attaccato e sfruttato. Una volta rilevato il firewall, gli avversari cercheranno delle vulnerabilità e le sfrutteranno per ottenere l'accesso. Dopo averlo ottenuto, potranno rubare i dati e negare l'accesso oppure potranno muoversi lateralmente verso altri dispositivi presenti sulla rete e cercare delle vulnerabilità.

Le architetture di sicurezza tradizionali non sono in grado di prevenire questi attacchi sofisticati. Quando un utente entra in una rete "sicura", che lo faccia in buona o cattiva fede, diventa automaticamente un utente attendibile, e ottiene l'accesso laterale a tutte le applicazioni, anche se non dovrebbe. I firewall virtuali sono rischiosi tanto quanto le loro controparti fisiche, perché anch'essi possono essere individuati e sfruttati per scagliare attacchi, spesso in numero maggiore rispetto ai firewall fisici, incrementando ulteriormente il rischio.

La maggior parte degli aggressori non attacca il primo dispositivo che incontra. Al contrario, l'utente malintenzionato effettua innanzitutto un'analisi dell'ambiente per determinare come muoversi lateralmente attraverso la rete per infettare altre risorse, e può spostarsi rapidamente e silenziosamente per depositare il ransomware in più di un sistema. Una volta raggiunta una massa critica, il ransomware cripta tutte le risorse contemporaneamente, gettando l'organizzazione nel caos. Questo accade a causa della natura piatta delle architetture di sicurezza della rete.

Come analogia, pensiamo a un ladro che entra in casa nostra passando dalla finestra del bagno. In bagno non c'è nulla da rubare, quindi si sposta nella camera da letto o in qualsiasi altra zona in cui siano conservati degli oggetti di valore; non c'è nulla che si possa fare per fermarlo, perché nessuna stanza è chiusa a chiave o dispone di altre protezioni.

Come prevenire le minacce informatiche con lo zero trust

Per mettere in sicurezza l'accesso alle applicazioni, è necessario eliminare la superficie di attacco dell'organizzazione e applicare la sicurezza inline e all'edge. Rendendo le app invisibili agli aggressori e accessibili solo agli utenti autorizzati, la superficie di attacco viene praticamente azzerata e l'accesso alle applicazioni su Internet, SaaS e nei cloud pubblici o privati è sempre sicuro.

In che modo lo zero trust affronta il movimento laterale delle minacce? Lo zero trust crea collegamenti diretti tra le entità autorizzate, ad esempio, collega un utente autenticato a un'applicazione specifica.

Il 67% delle organizzazioni concorda sul fatto che i firewall non siano in grado di fornire in modo efficace un accesso rapido e sicuro agli utenti in remoto[1]

Solo l'utente autenticato ha accesso all'applicazione richiesta, e nessun altro utente può accedervi. Questo significa che non è possibile individuare l'applicazione; in questo modo, non solo si elimina il percorso di attacco, ma si garantisce anche che le minacce non possano propagarsi lateralmente su altri dispositivi o applicazioni.

Riprendiamo l'analogia del furto in casa; in questo scenario, per il ladro è praticamente impossibile trovare la casa, perché senza una superficie di attacco la casa stessa non può essere individuata. Anche se in qualche modo riuscisse a trovarla, tutte le sue parti, che si tratti del bagno, del soggiorno o della camera da letto, sono indipendenti e scollegate le une dalle altre, in quanto ognuna ha un proprio accesso unico. In questo modo, il ladro non è in grado di spostarsi da una parte all'altra.

Con lo zero trust, i controlli vengono configurati per verificare l'identità e il contesto, e quest'ultimo viene controllato costantemente. Una soluzione zero trust dovrebbe essere in grado di decifrare tutti i dati, identificare le potenziali perdite di dati e impedire la ricezione di minacce. Viene stabilita una connessione sicura attraverso una serie di fattori contestuali e spaziali correlati all'utente che vengono convalidati continuamente, come la geolocalizzazione, l'indirizzo IP, il profilo del dispositivo e l'ora del giorno. Ciò avviene dietro le quinte, in modo che gli utenti autorizzati non siano interrotti mentre svolgono il loro lavoro.

N°2

Inefficienze operative dovute alla complessità

Una delle attività più impegnative nella protezione di un'organizzazione consiste nella distribuzione delle policy su infrastrutture diffuse, come infrastrutture cloud e hardware. Le aziende determinano la propria policy aziendale per designare dall'alto ciò a cui i propri dipendenti possono accedere. Queste policy aziendali vengono poi tradotte in policy della rete, poiché il modello di sicurezza perimetrale è dipendente dall'accesso alla rete. In un'infrastruttura distribuita, dove gran parte delle applicazioni non sono sul data center, ma su SaaS o cloud, e in cui gli utenti operano principalmente da remoto, l'applicazione delle policy di rete è complessa, perché il perimetro viene esteso oltre la semplice infrastruttura hardware del data center, e raggiunge tutte le posizioni in cui si trovano utenti e applicazioni. Pensiamo a un operatore che definisce le policy per una rete di questo tipo: le policy di accesso devono essere definite per quando l'utente è in ufficio, per le applicazioni SaaS, per i firewall, per IPS/IDS e molto altro. Si tratta di un'operazione praticamente impossibile.

Le applicazioni moderne non risiedono solo su un singolo cloud, ma possono avere dipendenze distribuite in un ambiente multicloud con cui devono comunicare spesso. La gestione delle applicazioni negli ambienti multicloud è particolarmente complessa rispetto alla creazione di una connettività sicura tra più cloud e data center. Bisogna combinare VPN da sito a sito, firewall, gateway di transito e policy di peering, che aumentano significativamente il livello di complessità.

Gli operatori di rete devono prevedere come si evolveranno le necessità ed eseguire importanti operazioni di capacity planning per soddisfare

Il 75% delle organizzazioni pensa che sia difficile gestire l'hardware, gli aggiornamenti e le distribuzioni dei firewall[1]

le esigenze future di larghezza di banda e di scalabilità. Sottostimare le esigenze di rete strozza le prestazioni, mentre sovrastimarle, al contrario, comporta costi inutilmente elevati e l'acquisto di apparecchiature che finiscono per rimanere inattive. Inoltre, vengono utilizzati numerosi prodotti che affrontano diversi aspetti della sicurezza in modo isolato, e questi richiedono un intervento periodico da parte dei team per gli aggiornamenti del software, la gestione delle patch, la risoluzione dei problemi, ecc. Queste attività sono fondamentali per garantire la sicurezza di un'organizzazione, ma possono richiedere settimane o addirittura mesi per essere eseguite.

Come ridurre la complessità con lo zero trust

Tra le entità che cercano di connettersi (come dispositivi mobili, IoT e altro) e le risorse a cui queste cercano di accedere (applicazioni SaaS, Internet e altro) si colloca un policy enforcer che applica le policy aziendali (che determinano ciò a cui i dipendenti possono accedere) e il contesto in una serie di modalità per prendere decisioni in merito alla concessione dell'autorizzazione; il policy enforcer quindi agisce da intermediario e autorizza la connettività alla risorsa richiesta. L'applicazione inline delle policy aziendali elimina la complessità della traduzione delle stesse in policy di rete, come avviene nei modelli perimetrali.

Una soluzione zero trust integrata protegge tutte le applicazioni SaaS, Internet e private sfruttando un'unica piattaforma, così non si deve pensare alla manutenzione e alla gestione di più soluzioni di sicurezza virtuali o basate su hardware. Una piattaforma zero trust unificata, con un'unica console di gestione, è molto più rapida da configurare, è più facile da gestire, semplifica le policy e offre una maggiore sicurezza rispetto alle soluzioni basate sulla sicurezza del perimetro.

Una soluzione zero trust in cloud colloca i controlli di sicurezza, gli utenti e le applicazioni sul cloud, e per questo è facilmente scalabile. Inoltre, se il volume degli utenti e le applicazioni aumentano, la scalabilità è garantita, e si è in grado di offrire un'esperienza utente uniforme, rapida e senza interruzioni. Grazie alla maggiore visibilità su utenti, cloud e carichi di lavoro, lo zero trust semplifica le operazioni e la risoluzione dei problemi.

N°3

Problemi di produttività e collaborazione a causa di un'esperienza utente scadente

Gli utenti si aspettano che le applicazioni funzionino quando ne hanno bisogno, che siano in sede, a casa o in viaggio. Non sono interessati al modo in cui si svolge l'accesso o al modello di rete e sicurezza del back-end. Quando le applicazioni non sono accessibili o sono lente a rispondere, la produttività diminuisce e la frustrazione aumenta.

L'architettura di rete hub and spoke richiede che le sedi in remoto e le filiali si colleghino all'ufficio centrale (data center) tramite firewall con MPLS e agli utenti in remoto con una VPN.

Aumento del **300%** dei dipendenti che lavorano da remoto[4]

Questa architettura crea una rete piatta che si estende a tutte le posizioni e prevede che tutto il traffico di rete sia indirizzato verso un set di strumenti di sicurezza centrale. L'invio del traffico da un utente in remoto al cloud passando per il data center, per poi tornare all'utente seguendo lo stesso percorso al contrario, aumenta significativamente la latenza e peggiora l'esperienza utente. Lo stesso problema riguarda anche i firewall virtuali. Anch'essi fanno parte dell'architettura di rete piatta che richiede che tutto il traffico venga indirizzato verso il firewall virtuale situato nel cloud, creando così un nuovo punto di strozzatura.

Per le organizzazioni è essenziale fornire la migliore esperienza utente possibile a tutti gli utenti, compresi dipendenti, partner, fornitori e clienti, in qualsiasi luogo, e su qualsiasi dispositivo. Ma questo può rivelarsi complesso per i team IT e di sicurezza, perché utenti, dati, applicazioni e dispositivi sono più distribuiti che mai.

Come migliorare l'esperienza utente con lo zero trust

Lo zero trust risponde ai problemi prestazionali degli utenti applicando le policy inline all'edge, in modo che non siano necessari ulteriori hop, e fornendo così connessioni dirette alle applicazioni indipendentemente dalla posizione dell'utente o dal dispositivo. Le connessioni dirette eliminano la necessità di effettuare il backhauling del traffico attraverso controlli di sicurezza centralizzati, che aggiungono latenza. Operando nel percorso dati, una piattaforma zero trust è in grado, inoltre, di monitorare ogni connessione e individuare e risolvere automaticamente i problemi prestazionali.

Una soluzione zero trust fornita all'edge esegue la scansione di tutti i contenuti in un unico passaggio, senza copiare pacchetti e aggiungere latenza. Questo approccio è decisamente diverso dal modello che prevede l'utilizzo di una catena di apparecchi fisici o virtuali, dove ogni servizio di sicurezza elabora i pacchetti in modo indipendente e aggiunge latenza a ogni hop. Con un'unica scansione, le policy possono essere applicate a vari motori di sicurezza con una latenza minima.

Le applicazioni UCaaS (Unified Communications as a Service) critiche, come Microsoft Teams e Zoom, richiedono basse latenze per poter funzionare in modo efficiente. Una soluzione zero trust efficace consente agli operatori di soddisfare queste esigenze di bassa latenza e alta disponibilità grazie al peering con le società delle applicazioni, per consentire la connessione diretta in base alla disponibilità e alla capacità dell'applicazione. Ad esempio, se un utente di M365 accede all'applicazione dal Texas, sarà connesso al data center più vicino e verrà eseguito un controllo di sicurezza inline. L'applicazione delle policy avviene inline, all'edge, senza la necessità di effettuare ulteriori hop; si tratta di un approccio rivoluzionario rispetto all'architettura hub and spoke.

Per incrementare la collaborazione e la produttività dei dipendenti, lo zero trust deve monitorare queste applicazioni e risolvere rapidamente i problemi, sfruttando la funzionalità di monitoraggio dell'esperienza digitale (Digital Experience Monitoring, o DEM). Con una soluzione inline che opera nel percorso dei dati, è molto più facile monitorare ogni connessione e individuare automaticamente e rapidamente i problemi nelle prestazioni.

N°4 Team IT isolati con conseguente rallentamento della trasformazione

Per trasformare il business bisogna trasformare anche l'IT. Tuttavia, il passaggio a una soluzione zero trust con base cloud e la sostituzione dell'infrastruttura hardware possono rivelarsi un compito estremamente arduo. Si tratta di una sfida sia per l'organizzazione che per i team IT addetti a varie funzioni, come sicurezza, reti e operazioni.

Uno dei principali ostacoli alla trasformazione digitale nelle organizzazioni è la mancanza di comunicazione all'interno dei team IT, che però non è intenzionale, e deriva dal fatto che questi team sono stati concepiti per lavorare su aree diverse dell'infrastruttura di rete e sicurezza. Il lavoro si concentra su singoli componenti, e non si ha una visione d'insieme quando si tratta di risolvere problemi generali. Questi team sono abituati a lavorare sulle soluzioni relative alle loro specifiche aree: ad esempio, il team della sicurezza installa i firewall, abilita le VPN e si assicura che il set di soluzioni di sicurezza sia attivo e funzionante, mentre il team delle reti si assicura che il routing e lo switching funzionino bene e che i protocolli, come MPLS, OSPF e altri, siano attivi. Questi due team di solito non collaborano, a meno che non si tratti di un problema di interoperabilità. L'ammodernamento dell'infrastruttura cloud richiede però che questi team cooperino, e questo rappresenta un grande cambiamento rispetto al loro modo tradizionale di operare. Questo cambiamento può essere difficile da realizzare se non si dispone della formazione, degli strumenti e dei processi giusti.

Il 67% dei professionisti della sicurezza pensa che lavorare nell'ambito della sicurezza sul cloud rappresenti una migliore opportunità di carriera a lungo termine rispetto alla gestione dei firewall[1]

In fondo, le organizzazioni hanno investito risorse nelle architetture di sicurezza esistenti, e hanno bisogno di un valido motivo per adottarne di nuove. Cambiare la mentalità dei team che promuovono la transizione verso il cloud si rivela spesso difficile, perché da decenni si tende a pensare alla sicurezza sempre nello stesso modo. Dal canto loro, gli operatori di rete che gestiscono da anni firewall e VPN, possono temere di non avere le competenze necessarie per lavorare con delle soluzioni di sicurezza cloud.

Come affrontare la trasformazione con lo zero trust

Una piattaforma cloud zero trust semplifica la gestione e le operazioni di sicurezza. I team addetti alla rete, alla sicurezza e alle operazioni possono lavorare insieme per allontanarsi dall'approccio basato sul perimetro e muoversi verso una soluzione basata sulle policy aziendali, che può trasformare l'infrastruttura esistente sfruttando una soluzione cloud zero trust. La riduzione del carico di lavoro consente ai team di utilizzare il nuovo tempo a disposizione per concentrarsi su progetti strategici, come l'analisi dei dati, l'ottimizzazione della sicurezza e altre attività che supportano più direttamente gli obiettivi aziendali. Le organizzazioni sono molto più al sicuro quando i team abbattono le barriere tra di loro, comunicano e collaborano.

Il passaggio a una soluzione cloud zero trust riduce inoltre il carico dei team IT relativamente all'acquisto, alla gestione, alla manutenzione e alla supervisione dell'hardware, e consente loro di avere più tempo a disposizione per portare avanti altri progetti. I CISO e i CIO non devono più prevedere accuratamente il futuro per calcolare i requisiti di hardware e i costi di consumo della larghezza di banda. Attraverso una comunicazione chiara e un piano solido, le organizzazioni possono guadagnare la fiducia e il supporto dei loro team IT e di sicurezza e portare a termine con successo la trasformazione cloud.

N°5 Costi infrastrutturali elevati a causa di distribuzioni inefficienti

L'infrastruttura di rete necessaria per supportare le architetture hub and spoke, che si basano su protocolli come l'MPLS, è costosa da acquistare e implementare e richiede un team IT esperto che si occupi della manutenzione. Prevede inoltre il costo aggiuntivo della larghezza di banda, dovuto all'inoltro del traffico al data center anche quando non è necessario, ad esempio quando si accede a un'applicazione SaaS su cloud. Al di là dell'infrastruttura di rete, il costo dell'infrastruttura di sicurezza, che comprende firewall, switch, bilanciatori di carico, controlli di accesso, VPN, sandbox e sistemi di prevenzione delle intrusioni, è elevato e va ben oltre il semplice prezzo di acquisto di queste tecnologie. Vanno infatti considerati anche i costi dell'installazione, della configurazione, del provisioning, dei test e della risoluzione dei problemi, oltre all'onere aggiuntivo della manutenzione finale di questi sistemi. Tutte queste spese si moltiplicano quando si adotta una molteplicità di prodotti diversi, ed è necessario ricorrere a personale altamente qualificato per garantirne il funzionamento.

I CIO e i CISO devono prevedere con precisione la capacità futura dell'organizzazione e stimare i requisiti di hardware e i costi di consumo della larghezza di banda dovuti all'invio di tutto il traffico al data center tramite MPLS per l'ispezione. Si tratta di un equilibrio delicato: sottostimare i requisiti e i costi potrebbe impedire all'azienda di riuscire ad adattarsi efficacemente alla crescita della domanda, mentre sovrastimarli comporterebbe spese inutili. Inoltre, sottovalutare le esigenze di rete potrebbe ostacolare la produttività, mentre sopravvalutarle potrebbe comportare costi elevati e portare all'acquisto di apparecchiature che rimarranno inutilizzate. Infine, ogni sede avrà probabilmente bisogno di distribuzioni uniche, e questo può portare all'accumulo di molteplici prodotti diversi nell'infrastruttura.

Per quanto riguarda il traffico diretto a Internet, ha più senso utilizzare connessioni a banda larga, il cui costo è comparabile a una piccola frazione dell'infrastruttura di sicurezza della rete; tuttavia, queste connessioni devono essere protette. Ma come fare per proteggerle? L'installazione di un gateway di sicurezza in ogni filiale per consentire connessioni dirette è altrettanto dispendiosa e complessa.

Il 50% di tutti i dati aziendali è archiviato sul cloud[2] e il

Il 70% delle applicazioni aziendali è basato su SaaS[3]

Come ridurre i costi con la trasformazione cloud zero trust

Passare a una soluzione zero trust nativa del cloud consente alle organizzazioni di ridurre i costi e migliorare al contempo la sicurezza, grazie all'eliminazione delle VPN, dei costi di transito sul cloud pubblico e delle architetture di rete su misura. Lo zero trust abbatte i costi esterni associati all'aumento degli accessi da remoto, mentre le organizzazioni che adottano soluzioni basate sul perimetro si trovano a dover adattare le prestazioni dei firewall e delle VPN esistenti andando incontro a costi elevati per gli apparecchi e per l'infrastruttura, che incidono pesantemente sul budget dell'IT.

Lo zero trust elimina la necessità di costose reti MPLS che richiedono operazioni complesse di routing, switching, segmentazione della rete e altro, e offre un accesso diretto, rapido e sicuro al cloud e una connettività affidabile da cloud a cloud. Inoltre, un'architettura zero trust con base cloud semplifica la sicurezza e riduce le tempistiche di distribuzione da mesi a giorni, contribuendo al contempo a rilevare, prevenire ed evitare onerose violazioni dei dati che potrebbero costare milioni all'organizzazione. Una soluzione cloud zero trust è molto più conveniente, facile e veloce da scalare per le aziende, le quali possono acquistare componenti o funzionalità in base alle proprie esigenze, senza dover pianificare in modo estensivo ed evitando di effettuare acquisti inutili.

Raggiungere il vero zero trust con Zscaler

Zero Trust Exchange di Zscaler offre lo zero trust sfruttando il security cloud più grande del pianeta per fornire connessioni veloci e sicure che consentono ai dipendenti di lavorare in modo sicuro da qualsiasi luogo e su qualsiasi dispositivo, utilizzando Internet come rete aziendale. A differenza dei firewall e delle VPN, Zero Trust Exchange si basa sul principio dell'accesso a privilegi minimi, ossia sul concetto che nessuna applicazione e nessun utente debbano essere automaticamente ritenuti attendibili. Le connessioni vengono invece autorizzate tramite policy aziendali che si basano sull'identità e sul contesto dell'utente. Una volta verificata e applicata la policy aziendale, Zero Trust Exchange agisce da broker e stabilisce la connessione tra le risorse. Gli utenti e i dispositivi vengono collegati direttamente alle applicazioni, e non alla rete aziendale.

Per saperne di più su Zero Trust Exchange: www.zscaler.it/platform/zero-trust-exchange

Guarda questo webinar e scopri perché i firewall non sono in grado di applicare lo zero trust:
info.zscaler.com/webinar-why-firewalls-cannot-do-zero-trust?utm_source=digital

Fonti:
[1]Virtual Intelligence Briefing (ViB) Networks Security Survey 2021
[2]Statista. Percent of data and sensitive data stored in the cloud worldwide.
www.statista.com/statistics/1202541/sensitive-data-cloud-location
[3]Better Cloud. (2021). The State of SaaSOps 2021.
stateofsaasops.bettercloud.com/?_ga=2.164919740.241347015.1636678142-1969514686.1636678142
[4]Grady, John. (2021). The State of Zero Trust Security Strategies. Enterprise Strategy Group.
https://info.zscaler.com/resources-industry-report-the-state-of-zero-trust-security-strategies

zscaler™ | Experience your world, secured.™

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 dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata su SASE, è la più grande piattaforma di cloud security in linea del mondo. Scopri di più su **zscaler.it** o seguici su **Twitter @zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it