E-book

L'azienda sicura incomincia dallo zero trust

Accelera la trasformazione del business

La sicurezza è alla base di una trasformazione di successo

La trasformazione digitale può aiutare l'azienda a raggiungere i propri obiettivi strategici, come l'ottenimento di vantaggi competitivi sostenibili, la leadership sul mercato, la creazione di nuovi modelli di business, la possibilità di sfruttare nuove opportunità di guadagno e molto altro. Tutto ciò, a patto che si disponga di una base sicura.

Tuttavia, le tecnologie fondamentali per la trasformazione, come cloud, mobilità, SaaS, Internet of Things (IoT) e altre soluzioni, possono incrementare significativamente il rischio di subire attacchi informatici dannosi. Il perimetro aziendale tradizionale non è sufficiente per proteggere le aziende in un mondo basato sul cloud, dove utenti, applicazioni e dati sono ovunque e, di conseguenza, la superficie di attacco è sempre più estesa. Gli approcci legacy alla sicurezza sono inadeguati negli ambienti cloud moderni, e portano a un aumento della complessità, dei costi e del carico operativo, creando ostacoli che ritardano la trasformazione.

È per questo motivo che le aziende devono rivoluzionare la sicurezza e porla alla base della trasformazione digitale. Il successo parte dalla sicurezza, e la sicurezza inizia dallo zero trust.

Ecco come fare.

Dire addio alle architetture legacy

L'approccio tradizionale alla sicurezza (noto come architettura a castello e fossato) punta a difendere il perimetro (cioè il fossato) per proteggere l'organizzazione (cioè il castello) dagli attacchi esterni. Le difese perimetrali proteggono la rete, e considerano tutto ciò che si trova al suo interno e all'interno del data center sicuro e attendibile.

Ma il mondo è cambiato:

- **Viviamo in un mondo cloud first:** ora il cloud è la nuova sede del lavoro, ha preso il posto del data center e sta diventano il nuovo centro gravitazionale delle aziende. Lo spostamento delle applicazioni verso il cloud è ormai in corso e l'utilizzo del SaaS continua a crescere. Quindi, come fanno le aziende a proteggere le proprie operazioni cloud se non sono più all'interno del castello?
- **Il traffico interno non può più essere ritenuto attendibile:** il perimetro si è ormai dissolto, perché la nuova realtà è fatta di dispositivi personali (BYOD), mobilità e lavoro da remoto. Gli attacchi informatici dannosi sfruttano l'attendibilità implicita, facendo leva sulle difese carenti a livello perimetrale. Le reti legacy piatte consentono il movimento laterale illimitato ad aggressori sempre più sofisticati, e questi ultimi si spostano da un utente infetto a un numero crescente di computer (o controller di dominio, server o carico di lavoro), mettendo a rischio l'intera rete.
- **Gli approcci di sicurezza legacy sono obsoleti:** nonostante il nome, che potrebbe suggerire il contrario, i firewall di nuova generazione (NGFW) e le altre soluzioni di sicurezza di rete legacy non sono stati progettati per l'architettura IT moderna e la trasformazione cloud, e non sono in grado di supportare lo zero trust, il modello di sicurezza più consigliato e basato sul contesto, che rimuove l'attendibilità implicita per proteggere utenti, dispositivi, applicazioni e dati, indipendentemente da dove si trovino. Gli NGFW e le altre soluzioni legacy sono troppo fragili, complessi e costosi per supportare efficacemente i principi dello zero trust, ridurre i rischi e proteggere al meglio l'azienda.

STATISTICHE SUI DATI

lo stato della sicurezza sul cloud

80%

dei principali attacchi hanno sfruttato i servizi esposti a Internet[1]

26%

dei server espone le proprie porte Secure Shell (SSH) a Internet[2]

20%

dei server espone le porte RDP (Remote Desktop Protocol) a Internet[3]

#1

preoccupazione dei CEO negli USA: le minacce informatiche[4]

63%

delle trasformazioni della sicurezza informatica sono in ritardo rispetto alla digitalizzazione o cercano solo di stare al passo[5]

Fonti: 1. NSA 2020; 2–3. Zscaler, "The 2020 State of Cloud (In)Security;" 4–5. PwC, "Cyber-ready — Today and for Tomorrow," giugno 2021

Comprendere le limitazioni della sicurezza tradizionale nel cloud

L'estensione di approcci di sicurezza tradizionali, come gli NGFW, ad ambienti cloud moderni, ibridi o multicloud comporta più problemi che vantaggi. Tra questi problemi, vi è l'estensione ulteriore della superficie di attacco, che pone l'azienda a un rischio persino maggiore.

Le organizzazioni utilizzano principalmente due approcci per adattare l'infrastruttura di sicurezza legacy al cloud: estendono la rete e l'infrastruttura di sicurezza al cloud, o ampliano il perimetro affinché includa il cloud. Nessuno di questi due approcci offre la solida sicurezza di cui le aziende hanno bisogno per accelerare la trasformazione digitale.

UTILIZZO DELLA SICUREZZA TRADIZIONALE IN UN MONDO CLOUD

APPROCCIO N. 1:
Estendere la rete legacy e la sicurezza al cloud

- Estendere la rete al cloud tramite VPN sito a sito
- Estendere la rete a tutti gli utenti tramite VPN
- Estendere la rete alle sedi delle filiali tramite MPLS

SFIDE

Scarsa esperienza utente.
Il backhauling del traffico introduce latenza e influisce negativamente sulle prestazioni delle applicazioni.

Rischio del movimento laterale delle minacce.
L'estensione della WAN incrementa i rischi. Un singolo utente infetto può diffondere malware in tutto ciò che è presente sulla rete aziendale.

Costi elevati e spese operative.
Con il proliferare del set di servizi della security, i costi incrementeranno di conseguenza.

APPROCCIO N. 2:
Ampliare il perimetro per includere il cloud

- Estendere la rete al cloud tramite VPN da sito a sito
- Estendere la rete agli utenti tramite VPN a cloud firewall virtuali
- Estendere la rete alle sedi delle filiali tramite VPN da sito a sito

SFIDE

Superficie di attacco estesa.
Tutte le applicazioni e tutti i firewall visibili su Internet possono essere individuati e potenzialmente sfruttati.

Rischio di movimento laterale delle minacce.
Il perimetro diventa estremamente ampio e, una volta ottenuto l'accesso, non c'è niente che fermi un aggressore.

Spese operative e costi elevati.
Sebbene questo approccio possa ridurre i costi MPLS, gestire un numero crescente di firewall e quantitativi enormi di avvisi dai firewall aumenta i costi e le spese operative.

La trasformazione della sicurezza inizia dallo zero trust

La trasformazione sicura richiede un approccio nuovo e innovativo, che reinventi la sicurezza nella sua totalità, affinché diventi la base della trasformazione. Questa base si può costruire con lo zero trust.

Lo zero trust è un approccio moderno alla sicurezza, che si basa sul principio dell'accesso a privilegi minimi e sull'idea che nessuna applicazione e nessun utente debbano essere considerati automaticamente attendibili. Un'architettura zero trust implementa questi principi per connettere in modo sicuro utenti, dispositivi e applicazioni utilizzando le policy aziendali.

Con una base sicura, costruita sullo zero trust, è possibile ottenere la sicurezza di cui l'azienda ha bisogno per accelerare la trasformazione. Per un'architettura zero trust che sia agile, trasparente, scalabile e semplice, non è possibile utilizzare NGFW, apparecchi di sicurezza e approcci di rete tradizionali. È necessaria una soluzione moderna e nativa del cloud.

Un'architettura zero trust

- Protegge dalle minacce informatiche sofisticate
- Previene la perdita di dati
- Previene il movimento laterale delle minacce
- Offre un'esperienza utente ottimale
- Riduce i costi e la complessità

Creare una base sicura con Zscaler

Per accelerare la propria trasformazione digitale sicura, le imprese più trasformative del mondo si sono affidate alla piattaforma di sicurezza più trasformativa del mondo. Zero Trust Exchange™ di Zscaler accelera la trasformazione aziendale e mette in sicurezza il cloud proteggendo utenti e applicazioni, indipendentemente dalla loro posizione, con l'identità basata sul contesto e l'applicazione delle policy.

A differenza degli NGFW e dei vari prodotti di sicurezza tradizionali, Zero Trust Exchange è una soluzione progettata per proteggere la forza lavoro ibrida e cloud first di oggi offrendo sicurezza in modo proattivo, intelligente e radicalmente semplice, e riducendo così il rischio aziendale.

Abbiamo creato l'unica vera piattaforma zero trust al mondo, rivoluzionando decenni di approcci legacy, astraendo la sicurezza dalla rete soggiacente per connettere in modo sicuro utenti e dispositivi direttamente alle applicazioni. Garantiamo che le minacce e i tentativi di furto dei dati vengano individuati, bloccati e contenuti, per consentire alle aziende di portare avanti il proprio business con fiducia.

Zero Trust Exchange è costruita su tre principi, il che la rende una soluzione di livello superiore

ZSCALER ZERO TRUST EXCHANGE

1. **Zero accesso alla rete.** Connetti gli utenti alle applicazioni, non alle reti aziendali, per impedire il movimento laterale.

2. **Zero superficie di attacco.** Rendi invisibili le applicazioni, in modo che non possano essere attaccate.

3. **Zero connessioni passthrough.** Nega tutti i privilegi utilizzando la nostra architettura proxy, per una migliore difesa dalle minacce informatiche e per proteggere i dati.

CASTELLO E FOSSATO/APPROCCIO BASATO SUL PERIMETRO

Accesso alla rete. Gli utenti vengono connessi alle reti per l'accesso alle applicazioni.

Superficie di attacco estesa. Le applicazioni vengono pubblicate su Internet, e questo estende la superficie di attacco.

Connessioni passthrough. L'architettura firewall passthrough offre una capacità limitata di ispezione del traffico e di protezione dei dati.

PERCHÉ SCEGLIERE ZSCALER?

Ridurre il rischio grazie alla nostra architettura proxy

Zero Trust Exchange utilizza un'architettura proxy in grado di ispezionare le sessioni SSL, analizzare i contenuti all'interno delle transazioni e prendere decisioni in tempo reale su policy e sicurezza. Questo approccio proxy interrompe completamente la connessione e, in seguito, la ristabilisce.

A confronto, un approccio basato sulla sicurezza di rete tradizionale o un firewall utilizza una connessione passthrough che non è in grado di eseguire un'ispezione adeguata per la sicurezza e la protezione dei dati, e consente alle minacce 0-day di infettare le organizzazioni.

PRINCIPIO N. 1

Prevenire la compromissione bloccando le minacce prima che raggiungano l'azienda

Invece di estendere la superficie di attacco con la trasformazione cloud, Zero Trust Exchange rende le applicazioni invisibili e la elimina completamente. Allo stesso tempo, utenti, server, applicazioni e sistemi IoT/OT vengono protetti grazie a una piattaforma che offre tutti i controlli di sicurezza aziendali critici come servizio all'edge, vicino a tutti gli utenti.

Con Zscaler, è possibile prevenire la compromissione:

- Rilevare, prevenire e contenere all'istante i più sofisticati attacchi e tentativi di attacco ransomware inline, in tutto il traffico, incluso quello SSL, grazie ai migliori servizi di sicurezza basati sull'intelligenza artificiale
- Interrompere gli attacchi con policy zero trust autonome, che si adattano continuamente al panorama delle minacce in continua evoluzione, con il supporto degli esperti di livello mondiale di Zscaler ThreatLabz e dell'intelligence sulle minacce, del security cloud più grande del mondo
- Impedire agli aggressori di individuare, sfruttare o infettare utenti e applicazioni, rendendo queste ultime invisibili a Internet e accessibili solo agli utenti o ai dispositivi autorizzati tramite Zero Trust Exchange
- Monitorare, convalidare e risolvere automaticamente le lacune nelle autorizzazioni, nelle policy di sicurezza e nella conformità, causate da errori di configurazione e dall'accesso troppo permissivo, in tutti gli ambienti cloud

PRINCIPIO N. 2

Evitare il movimento laterale e bloccare la diffusione

Il movimento laterale rappresenta uno dei maggiori rischi per la sicurezza delle reti aziendali tradizionali. Una volta che il malware si diffonde sulla rete, può propagarsi liberamente all'interno dell'organizzazione, causando danni diffusi.

Grazie a Zscaler, si elimina il rischio che si verifichino movimenti laterali, collegando direttamente utenti e dispositivi alle applicazioni, non alla rete. Utilizzando Zscaler, l'organizzazione è in grado di:

- Mitigare il danno potenziale dovuto a utenti o dispositivi compromessi, grazie alla funzionalità ZTNA integrata di Zscaler, per gli utenti in remoto e on-premise
- Estendere la prevenzione del movimento laterale basata sullo zero trust ai carichi di lavoro cloud e ai data center, attraverso una microsegmentazione innovativa che si fonda sull'identità, e che consente o blocca le comunicazioni dei carichi di lavoro negli ambienti ibridi e cloud
- Rilevare, bloccare e analizzare gli attacchi attraverso applicazioni fittizie ed esche proattive che generano avvisi altamente attendibili e forniscono informazioni critiche sulle sequenze di attacco

PRINCIPIO N. 3

Prevenire la perdita dei dati

Bloccare la perdita di dati causata dall'esposizione accidentale o dall'esfiltrazione dolosa, grazie alle funzionalità olistiche di protezione dei dati di Zscaler, che coprono dispositivi gestiti e non, server, cloud pubblico e applicazioni cloud. Grazie alla piattaforma Zscaler, l'azienda è in grado di:

- Controllare le applicazioni cloud autorizzate e non, garantendo al contempo la protezione dei dati sensibili inattivi dal furto o dall'esposizione accidentale, grazie alle funzionalità CASB più all'avanguardia del settore
- Tutelare i dati sensibili in movimento, attraverso controlli granulari di DLP che identificano e bloccano in tempo reale la perdita o il furto dei dati in tutto il traffico inline ed SSL
- Estendere i controlli di DLP ai dispositivi non gestiti e personali (BYOD), grazie all'esclusiva tecnologia integrata di Cloud Browser Isolation
- Individuare e correggere gli errori di configurazione pericolosi all'interno di SaaS e cloud pubblici, per prevenire le violazioni del cloud e la perdita di dati

La trasformazione della sicurezza inizia dallo zero trust

Accelera in sicurezza il passaggio al cloud
con Zero Trust Exchange di Zscaler.

Per saperne di più

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 sull'SASE, è la più grande piattaforma di cloud security inline 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