Il futuro della connettività è senza rete

Nell'ambito del loro costante percorso di trasformazione digitale, molte aziende stanno iniziando a valutare il modo in cui connettere i collaboratori ai dati e alle macchine. Per molto tempo, la modalità standard di fornire connettività è stata quella di assegnare semplicemente l'accesso a una rete, a tutti e in egual misura. Ma poi è intervenuta la sicurezza limitando l'accesso con l'uso di policy per le applicazioni, gestite sul perimetro della rete.

Oggi i dati, le applicazioni e le persone risiedono spesso al di fuori dell'infrastruttura di rete delle aziende. Ciò aggrava il problema dell'accesso, in quanto le aziende cercano disperatamente di capire chi deve connettersi a quali risorse e da quale posizione. Ad aumentare la complessità sono sia le persone sia le macchine che ora devono interagire tra loro; di conseguenza, tali requisiti di connettività non possono essere gestiti allo stesso modo. Nel tentativo di semplificare la propria infrastruttura di connettività, molte aziende si orientano verso un framework Zero Trust, per connettere persone e dispositivi in modo sicuro, senza dover coinvolgere la rete a un tale livello. Al contrario, la rete diventa un livello sottostante su cui le aziende definiscono le varie forme di connettività grazie al software.

Invece che consentire ai dipendenti un ampio accesso alla rete, l'approccio Zero Trust permette alle aziende di fornire un accesso protetto via Internet solo alle applicazioni o a risorse particolari di cui i singoli hanno bisogno. Possiamo distinguere due categorie di tipi di accesso. La prima consente al personale di accedere al web e alle applicazioni SaaS (Software as a Service), ecc. direttamente tramite Internet. La seconda fornisce l'accesso alle risorse interne ospitate nel data center o nel cloud pubblico, sempre tramite Internet. Poiché la rete aziendale separata non è più necessaria (o lo è molto meno) per entrambe le opzioni, un modello Zero Trust diventa funzionale per la sicurezza e per la connettività.

Una minor complessità infrastrutturale

Nel tentativo di ridurre ulteriormente la complessità della rete tradizionale, molte aziende inizieranno a chiudere i propri data center e a migrare le proprie risorse nel cloud pubblico. Il motivo è che non solo è più facile amministrare le infrastrutture cloud, ma questo modello offre anche la flessibilità di scalare le architetture in base alle esigenze aziendali. Con il modello SaaS, i clienti pagano un servizio e il team IT non deve più gestire manualmente le operazioni IT correlate. Lo stesso vale per i diversi componenti (rack, stack, energia) nei data center on premise delle aziende: una volta che le applicazioni sono state migrate nel cloud, i fornitori di servizi si occupano dell'amministrazione di tutte le risorse di calcolo.

Oggi la maggior parte delle aziende si affida ancora a diverse appliance per instradare il traffico est-ovest verso le filiali e le consociate, ma questo modello diventerà presto obsoleto. Il passaggio a infrastrutture cloud con modelli di lavoro ibridi offre al personale la libertà di lavorare ovunque. Negli scenari di lavoro ibrido, i singoli hanno solo bisogno di un accesso fidato per connettersi alle applicazioni di cui hanno bisogno, utilizzando l'identità per implementare l'accesso basato su policy a livello di applicazione. In questo scenario, la rete tradizionale diventa obsoleta.

I futuri protagonisti del mercato si adatteranno a questo nuovo approccio alla connettività molto più facilmente dei marchi già affermati. Dal momento che non hanno mai dovuto creare un'infrastruttura basata su hardware per avviare la loro attività, si affideranno a Internet naturalmente. Per rimanere competitive, le aziende affermate dovranno seguire l'esempio e abbandonare la rete.

Problemi di sicurezza in un mondo post-appliance

Molte aziende hanno affrontato troppo a lungo le complessità della sicurezza e del networking come un problema da risolvere. La connettività di rete è stata utile ai team IT per molto tempo, ma ha avuto anche alcuni impatti negativi sulle aziende, uno dei quali è la possibilità per i criminali informatici di diffondere più facilmente le minacce. Nonostante ciò, c'è ancora resistenza all'abbandono della connettività legata all'infrastruttura fisica. Affinché ciò avvenga, è necessario un cambiamento di

mentalità a livello di leadership, accettando che le nuove infrastrutture cloud portino con sé modalità di connessione che non si basano sulla rete. Parallelamente, i responsabili della sicurezza IT dovranno accettare il concetto di non avere un dispositivo fisico legato al perimetro della rete per un particolare scopo di sicurezza.

Poiché in passato i team di rete e di sicurezza si sono trovati in disaccordo in termini di priorità, una più stretta collaborazione tra le due funzioni è un buon punto di partenza per superare le preoccupazioni su come potrebbe essere la sicurezza in un mondo post-appliance e portare le infrastrutture verso il futuro. Ma una parte della soluzione consiste anche nello sviluppo da parte di entrambi i gruppi di una migliore comprensione di cosa significhi utilizzare l'identità per determinare l'accesso piuttosto che la semplice connettività di rete. Il modello Zero Trust può servire a entrambi gli scopi: sicurezza e connettività. Con una piattaforma Zero Trust basata su cloud, le applicazioni sono accessibili agli utenti da qualsiasi luogo e non sono visibili a Internet e, di conseguenza, ai criminali informatici.

I micro tunnel verso l'esterno tra il singolo utente e il punto di accesso, e tra quest'ultimo e l'applicazione pertinente sono uniti dalla piattaforma di sicurezza in base alle policy e all'identità dell'utente. Ciò significa che solo gli utenti autorizzati e autenticati possono accedere all'applicazione richiesta, a livello granulare. Grazie a questo meccanismo di sicurezza Zero Trust, le applicazioni non sono esposte a Internet e ai criminali informatici che non possono perciò sferrare i loro attacchi.

Il concetto di Zero Trust non solo elimina gli effetti negativi della connettività di rete (movimento laterale di malintenzionati), ma anche una serie di ulteriori effetti positivi. Innanzitutto, consente agli utenti di lavorare da qualsiasi luogo e di accedere a dati e applicazioni in modo sicuro, indipendentemente dal luogo in cui sono ospitati. Inoltre, grazie a un percorso di accesso diretto senza dover passare attraverso una rete aziendale, il modello Zero Trust può avere un effetto positivo sull'esperienza degli utenti, riducendo la latenza. Sia che un membro del personale lavori da casa o dall'ufficio, sia che si sposti da un ufficio all'altro, la sua esperienza (e il livello di sicurezza) rimane invariata.

L'intelligenza artificiale semplifica i criteri di accesso

L'unica sfida che le aziende devono affrontare è la definizione dei diritti e dei criteri di accesso. Per sapere chi può accedere a cosa all'interno di un'infrastruttura aziendale, è necessario avere una chiara visione delle applicazioni e dei vari gruppi di utenti e funzioni aziendali. Un'azienda standard con 10.000 utenti avrà la possibilità di raggruppare il personale in base alle funzioni o ai reparti come punto di partenza. Poi comincerà a stabilire eccezioni su ciò a cui i singoli hanno necessità di accedere, in base a esigenze funzionali trasversali o a ruoli specifici all'interno dell'organizzazione. Tuttavia, sarà più difficile delineare il quadro del panorama applicativo in uso all'interno dell'azienda stessa.

A questo punto entra in gioco l'intelligenza artificiale per generare le informazioni dettagliate necessarie sull'azienda come base per la generazione delle policy. La capacità di sviluppare mappe di ciò a cui le persone si collegano e di come utilizzano determinati software è ciò che differenzia un processo automatizzato dal mero onere amministrativo umano. Sulla base di queste informazioni, l'intelligenza artificiale può essere utilizzata per generare una prima serie di policy da sottoporre alla verifica umana per accelerare il processo di sicurezza Zero Trust.

Previsioni del settore

Il futuro della connettività sarà senza rete, ma la tempistica dipende dal settore in questione. Alcune aziende sono già in grado di migrare dal data center, mentre altre dovranno ancora eseguire internamente per un certo periodo le applicazioni principali, il che porterà a modelli ibridi. Tuttavia, tutte le aziende saranno in grado di riconoscere i vantaggi della migrazione dei loro processi nel cloud.

Che si tratti di evitare i costi elevati, la complessità amministrativa o la mancanza di flessibilità, un numero sempre maggiore di aziende sta pensando di abbandonare in via definitiva i propri data center. Coloro che lo hanno fatto sperimenteranno già la connettività senza rete, approfittando della facilità di connessione sicura da qualsiasi luogo a qualsiasi dispositivo, che è poi il vero obiettivo del modello Zero Trust.

A proposito di Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti da attacchi informatici e dalla perdita di dati collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange, basata su SSE, è la più grande piattaforma di sicurezza cloud in line del mondo.

Per ulteriori informazioni:

Tania Acerbi

Monica Fecchio

Prima Pagina

Piazza Giuseppe Grandi 19 - 20129 Milano

e-mail: tania@primapagina.it

e-mail: monica@primapagina.it