Axians

Smart Working: evoluzioni in cloud

Come estendere al cloud le applicazioni e l'architettura della loro sicurezza

La pandemia ha sicuramente avuto un effetto drammatico e ha dato una forte accelerazione allo smart working, una tendenza in atto da diversi anni, poiché le organizzazioni si stavano già spostando progressivamente verso una nuova tipologia di spazi di lavoro "ibridi".

Con tutti questi lavoratori da remoto, dispositivi IoT e ambienti cloud, si dovrà estendere la sicurezza della rete dall'edge al cloud, mantenendo elevata la produttività di tutti.

È importante, quindi, servirsi di una rete con visibilità, controllo e applicazione delle politiche basata su architetture Zero Trust, che permetta di applicare gli stessi controlli tanto alla infrastruttura centrale quanto a quelle delle filiali, agli uffici domestici e ai lavoratori da remoto, eliminando la necessità di VLAN generate manualmente che possono lasciare la porta aperta a potenziali rischi.

Con l'aumentare del numero di applicazioni migrate sul cloud, le organizzazioni devono pensare a come estendere al cloud l'architettura della loro sicurezza senza rifarsi al modello attualmente in uso. Il controllo degli accessi basato sull'identità a livello di rete dovrà essere combinato e integrato con i servizi di un fornitore di sicurezza del cloud.

Emiliano Gallo head of solutions consulting & software factory, Axians Centro-Sud Italia

Con una sicurezza intelligente e fornita dal cloud si potrà proteggere ogni utente, inclusi gli utenti remoti e mobili, da tutte le minacce, con semplicità e scalabilità, consentendo agli utenti di accedere alle applicazioni utilizzando l'accesso diretto a Internet (DIA) senza compromettere le prestazioni.

Una strategia Secure Access Services Edge (SASE) è sinonimo di Zero Trust Edge (ZTE) e le aziende di dimensioni più grandi, che hanno requisiti più complessi e servizi più eterogenei, sceglieranno un approccio multivendor anche perché l'attuale impiego di applicazioni legacy rende meno probabile l'adozione di un approccio basato su un singolo fornitore.

Ci sono però alcuni ostacoli da affrontare:

- **Applicazioni e servizi legacy**: non sempre è semplice configurare le applicazioni comuni basate su protocolli non Web, in particolare RDP/VDI e SIP/VoIP, per cui non esiste un metodo standardizzato di utilizzo nell'ambiente ZTE.
- **Dispositivi di rete esistenti**: oltre il collegamento di laptop, server e applicazioni allo ZTE, i team di networking e cyber-security dovranno collaborare per collegare tutti i dispositivi, su cui non può essere installato alcun agente software, utilizzando protocolli di rete accettati.
- **Protezione investimenti**: le aziende che hanno già effettuato ingenti investimenti nei loro data center per i servizi di sicurezza e networking ad alta capacità attenderanno il momento in cui dovranno migrare al cloud le loro applicazioni di importanza critica.

Axians, con il suo approccio innovativo, è partecipe di questo cambiamento perché innovare, per noi, significa pensare e agire in un modo nuovo, focalizzandoci sempre sulla cybersecurity aziendale, un elemento strategico per difendere le attività dal rischio costante di un attacco informatico, che spesso si traduce in importanti perdite economiche.