Migrare verso il cloud in sicurezza

La scelta di un modello di business e di delivery flessibile e dinamico come quello del cloud è oramai diventata imprescindibile. Il cloud, infatti, rappresenta il modo migliore per poter indirizzare le necessità di scalabilità e ottimizzazione di risorse necessarie per garantire e supportare la crescita delle aziende. Allo stesso tempo però le direttive sulla privacy e il cybercrime suggeriscono che la sicurezza debba essere un elemento di discussione se si decide di migrare i servizi verso il cloud.



Secondo l'Osservatorio Exprivia di CyberSecurity, sono 20 gli incidenti e attacchi subiti da piattaforme cloud nel corso del 2020 senza contare che molti incidenti classificati su tipi di industria diversi sono comunque assimilabili ad utilizzo di piattaforme cloud.

Pertanto migrare al cloud è necessario, ma è ugualmente necessario fare attenzione alla sicurezza. Ecco alcune semplici raccomandazioni.

Fare attenzione a direttive e regolamentazioni

Migrando dei servizi verso il cloud non è inusuale che dati dapprima processati in una definita e unitaria infrastruttura fisica, possano essere processati, immagazzinati o trasmessi tra diversi cloud che risiedono su diverse infrastrutture fisiche. In diverse nazioni ci sono delle restrizioni su dove i dati di un determinato tipo debbano essere immagazzinati. Senza un contratto specifico che costringa il fornitore ad immagazzinare i dati in una nazione specifica o dia visibilità

di dove i dati vengano immagazzinati, l'utilizzatore del servizio non avrà visibilità di dove il dato è stato immagazzinato o da dove il servizio viene erogato. Conoscere le regolamentazioni e direttive è fondamentale, tuttavia non è sufficiente. Infatti, le direttive e regolamentazioni potrebbero cambiare repentinamente. Se si sono fatti diversi investimenti per creare una infrastruttura che si basa su determinate regolamentazioni e direttive, si corre il rischio di dover vanificare gli investimenti a causa di un cambio di direttive e regolamentazioni. La nuova infrastruttura disegnata per il cloud pertanto deve essere sufficientemente flessibile da poter essere adattata in funzione del cambio delle regolamentazioni o direttive.

La segmentazione

Sembra paradossale parlare di segmentazione parlando di migrazione al cloud, ma invece questo tema resta uno dei più critici da prendere in considerazione per due ragioni. La prima è che la migrazione al cloud non riduce la necessità di segmentazione (ad esempio per i motivi legati alle regolamentazioni e direttive). La seconda è più intrinsecamente legata al concetto di migrazione. Infatti, se una applicazione viene sviluppata sul cloud, allora può essere opportunamente segmentata. Se invece la applicazione viene migrata da una infrastruttura fisica on premise, questa è stata sviluppata tenendo conto della segmentazione fisica su cui è stata sviluppata. Tutte le policies di sicurezza fanno spesso riferimento ad elementi infrastrutturali che fanno riferimento alla segmentazione fisica. Portare le policies nel cloud potrebbe comportare la necessità di studiare come reintrodurre le stesse policies in un ambiente in cui i riferimenti alla segmentazione fisica non sono più gli stessi. Questo vuol dire analizzare processi e tecnologie e spesso ridisegnare i controlli di sicurezza.

Microsegmentazione

Una risposta alle necessità di flessibilità e migrazioni di policies di sicurezza verso il cloud è la microsegmentazione (o segmentazione fatta a livello applicativo). Se la segmentazione (e cioè l'insieme di regole che assicurano il controllo di chi sta comunicando con chi) divide la rete in sottoreti, la microsegmentazione fa la stessa cosa ma a livello applicativo aumentando quindi la granularità su cui poter definire le policies e rendendo meno necessario il dover fare affidamento ad elementi che fanno parte della segmentazione fisica.

Non si parla più pertanto di segmenti di reti (normalmente che fanno affidamento sul Livello 4 dello stack OSI), ma di contenitori che possono includere ambienti di test o sviluppo o possono fare riferimento a regolamentazioni, applicazioni (e quindi oltre il livello 4 dello stack OSI fino al 7).

A parte la migrazione al cloud, gestire le policies di sicurezza facendo affidamento solo alla segmentazione fisica diventa sempre più necessario a causa della crescente complessità delle applicazioni stesse. Pertanto la microsegmentazione, che semplifica la migrazione al cloud indirizzando temi come flessibilità e portabilità delle policies di sicurezza, diventa sempre di più una buona pratica da adottare anche sulle infrastrutture totalmente on premise o ibride.

Ulteriore vantaggio della microsegmentazione è quello che tecniche di attacco che si basano sulla rete (ad esempio IP spoofing o tentativi di esecuzione su porte autorizzate) diventerebbero meni efficaci. Perlomeno l'attaccante avrà la necessità di superare molteplici livelli di sicurezza (sulle applicazioni possono essere create un numero molto elevato di policies).

Articolo a cura di **Domenico Raguseo**

https://www.ictsecuritymagazine.com/articoli/migrare-verso-il-cloud-in-sicurezza/