Le previsioni di cloud security per il 2019

Author : Redazione

Date : 29 Gennaio 2019

Le aziende hanno tratto vantaggio dalla flessibilità e innovazione offerte dalle piattaforme public cloud. Tuttavia, l'adozione di questi servizi può anche amplificare i rischi di sicurezza e le sfide di compliance se non viene pianificata con sufficiente attenzione.

Quindi, come si svilupperanno questi trend nei prossimi mesi? Ecco alcuni spunti:

La compromissione degli account aumenterà in termini di scala e velocità

La compromissione di credenziali sta diventando molto comune nel public cloud. Infatti, i ricercatori della Unit 42 hanno esaminato le minacce alla sicurezza cloud nuove ed esistenti tra maggio e settembre 2018 e hanno trovato che il 29 percento delle organizzazioni ha subito potenziali compromessi. Questa statistica è resa ancora più preoccupante dal fatto che il 27 percento di queste ha consentito anche attività root user. Quando un root cloud account viene compromesso, il cyber criminale ottiene accesso completo a quasi tutto ciò che si trova nell'account cloud. Le imprese devono necessariamente applicare una governance robusta e l'igiene degli accessi, oltre a operare in base al presupposto che la compromissione degli account è inevitabile. Partendo da un principio di breach presunto, le imprese possono focalizzarsi su un monitoraggio che identifichi e rapidamente intervenga in caso di attività utente sospette.

I container spopolano ma non sono sicuri per default

Non c'è dubbio che i container stiano rapidamente prendendo piede in azienda. La nostra ricerca Unit 42 rivela che una organizzazione su tre si avvale di orchestrazione Kubernetes nativa o gestita. Anche se AWS, Azure e Google svolgono la maggior parte delle attività legate ai servizi container gestiti, i consumatori di servizi public cloud devono fare la loro parte per quel che concerne la sicurezza. Un'area di estrema importanza è la sicurezza di rete, Unit 42 ha trovato che il 46 percento delle imprese abilita il traffico proveniente da qualunque fonte verso i loro pod Kubernetes, il che non è una pratica positiva.

Gli standard/benchmark della sicurezza public cloud diventeranno mainstream

I team dedicati alla sicurezza dedicavano mesi alla redazione di standard per la sicurezza cloud. Tutto ciò dovrebbe essere più semplice nel 2019. Lo scorso anno, il Center for Internet Security (CIS) ha completato i security benchmark per tutte le principali piattaforme public cloud infrastructure evitando così ai team di cybersecurity da farli e di doverli mantenere a mano a mano che i cloud provider rilasciano nuove funzionalità. E anche se non c'è la soluzione perfetta per la sicurezza cloud, questi standard possono servire da base condivisa e ridurre in modo significativo molti dei problemi di sicurezza cloud che hanno afflitto le imprese lo scorso anno.

Il cloud passa da iniziativa CIO a requisito del consiglio di amministrazione

Per molti anni l'utilizzo del cloud è stato frammentato per business unit. Nel 2018, i CIO hanno considerato il cloud come iniziativa a livello organizzativo, tuttavia oggi la maggior parte delle aziende riconosce che il cloud permette loro di innovare più rapidamente. Considerano quindi il passaggio alla nuvola un differenziatore. Nel 2019, vedremo i CdA chiedere a CIO e CISO di adottare iniziative cloud organization-wide e terranno d'occhio i loro team di tecnologia e cybersecurity per assicurarsi che la migrazione al cloud diventi realtà.

Quindi, se pensavate che il 2018 fosse stato un anno rivoluzionario per il public cloud, aspettate a vedere cosa ci riserva il 2019. Fate un grosso respiro, focalizzatevi, allacciate le cinture e preparatevi per un viaggio emozionante!

A cura di **Attila Narin***, European CTO and VP of Systems Engineering, Palo Alto Networks*