Cloud aziendale: sei aspetti a cui prestare la massima attenzione

OVHcloud

vmware®

Il Cloud computing è ormai legato indissolubilmente all'IT. Man mano che la trasformazione digitale conquista tutti i settori, le organizzazioni si stanno rivolgendo sempre più a strategie multi-Cloud per adeguarsi alle nuove esigenze di mercato. Per le aziende, un elemento fondamentale di questa strategia è il Cloud privato, considerato, per sua natura, più sicuro del Cloud pubblico[1].

Sebbene un Cloud privato aziendale offra un maggiore controllo dell'ambiente fisico e capacità di automazione impareggiabili, a esso sono associati alcuni aspetti fondamentali da tenere a mente.

Violazioni alla sicurezza

Violazioni dei dati, credenziali compromesse, broken authentication, interfacce e API hackerate: il 2018 non si è fatto mancare nulla in termini di violazioni alla sicurezza. I report settimanali di cyberattacchi e violazioni non aiutano certo a diminuire le preoccupazioni suscitate dal Cloud computing.

Questo induce molte aziende a pensare che i loro dati siano i più sicuri internamente, nei loro ambienti Cloud personalizzati. In realtà, gli ambienti ospitati sono tanto sicuri quanto quelli on-premise, se non di più. Sono concepiti e gestiti da esperti di sicurezza che comprendono le sfide della sicurezza Cloud e sanno come affrontarle.

Attacchi DDoS

Gli attacchi DDoS continuano a destare preoccupazione per tutte le aziende digitali. Nel corso degli anni, i responsabili di questi attacchi hanno elaborato metodi sempre più sofisticati e a causa delle nuove tecnologie, come l'Internet of Things, sono comparse nuove minacce.

Un attacco DDoS sovraccarica un server Web e può riuscire a rendere un sito inaccessibile per ore o addirittura giorni. Ciò può comportare un mancato guadagno e la perdita di fiducia da parte del cliente. Ne consegue che la protezione contro gli attacchi DDoS non è più una funzionalità accessoria: è un sistema di sicurezza cruciale. Tuttavia, la protezione on-premise non potrà mai essere efficace come quella dei sistemi leader del mercato di limitare gli attacchi.

[1] *Infobrief IDC, giugno 2019.*

“In qualità di provider di servizi Cloud, riceviamo e contrastiamo più di 2.000 attacchi DDoS al giorno. Il nostro sistema anti-DDoS protegge di default tutti i clienti. La ragione è molto semplice: un attacco DDoS, se non viene gestito, può provocare danni collaterali. Ciò significa che chi ne subisce le conseguenze non è solo l’obiettivo dell’attacco, ma anche tutti i server del rack. Il VAC (una combinazione di tecnologie sviluppate da OVHcloud per ridurre gli attacchi DDoS) si attiva solo quando viene rilevato un attacco. Tuttavia, per i clienti con esigenze specifiche in materia di sicurezza, proponiamo un filtro costante del traffico; in altre parole, un'attivazione permanente del VAC.”

Jakub Słociński, Network Innovation Manager di OVHcloud.

Sicurezza fisica e ridondanza

La maggior parte delle aziende non dispone delle stesse funzionalità di sicurezza fisica dei datacenter di terzi, il che può mettere in pericolo i loro dati sensibili. Un datacenter affidabile è come una fortezza, con un accesso rigorosamente controllato e una recinzione in filo spinato. I sistemi di videosorveglianza e di rilevazione del movimento devono essere in continuo funzionamento, così come i sistemi di rilevazione degli incendi e di estinzione.

Attualmente, l'accessibilità permanente, la disponibilità elevata e la resilienza sono elementi chiave per molti servizi IT. Raggiungere lo stesso livello di ridondanza per un Cloud privato interno sarebbe un compito arduo. I doppi alimentatori, i generatori di alimentazione, i dispositivi UPS e i collegamenti di rete ridondanti si aggiungono agli elevati costi di manutenzione. Non dimentichiamo inoltre la necessità di disporre, internamente, di un elevato livello di competenze.

.

Esigenze di conformità

Lo standard PCI DSS indica oltre 250 parametri di controllo e sicurezza da applicare per una gestione sicura dei dati delle carte bancarie. Un Cloud privato offre un maggior controllo sulla sicurezza, ma non rende più facile adeguarsi alle normative.

La conformità deve essere sempre una priorità, in particolare quando sono in gioco diversi tipi di dati regolamentati, come i dati sulle carte di pagamento, le informazioni aziendali sensibili e i dati dei clienti. Si tratta di un processo che richiede non solo tempo e denaro, ma anche la consulenza di un esperto IT che conosca le normative. Inoltre, il team IT dovrà sorvegliare costantemente i sistemi, sviluppare procedure chiare in caso di incidenti di sicurezza e utilizzare la cifratura dei dati per garantire il rispetto costante dei requisiti di conformità.

Performance

Le performance sono un problema ben noto negli ambienti virtualizzati dinamici. È difficile prevedere come qualsiasi modifica a livello dell'infrastruttura influenzerà le performance delle applicazioni, dato che anche un semplice aggiornamento del software può avere un impatto su un ecosistema chiuso. Per garantire un utilizzo ottimale della tua infrastruttura, è fondamentale implementare un processo continuo per confermare le performance del Cloud. Per ogni nuovo deploy e cambiamento importante, è necessario un test di performance realistico, preferibilmente automatizzato, che possa rilevare da subito i problemi. Questo processo permette di evitare spese inutili e di mantenere uno stretto controllo sul rapporto prezzo/performance.

Acquisto eccessivo di capacità

Che tu costruisca il tuo Cloud privato con OpenStack o VMware, la sfida è sempre la stessa: come ottenere flessibilità e scalabilità nella gestione di un'infrastruttura interna?
A livello di manutenzione dell'infrastruttura, un aumento di capacità richiederà più apparecchiature hardware. Quando non sono in grado di prevedere con precisione le capacità di cui avranno bisogno, i team IT spesso ne acquistano in eccesso, per assicurarsi di poter fornire le risorse necessarie al momento opportuno. Di conseguenza, i costi di investimento sono elevati e le prospettive di scalabilità ridotte.

Ci si può chiedere se un'infrastruttura on-premise possa davvero diventare "Cloud", perché il Cloud è caratterizzato da flessibilità e scalabilità, senza dover investire in hardware aggiuntivo. Tuttavia, anche se si potrebbe pensare che Cloud privato significhi semplicemente "on-premise", non è necessariamente così. Un Cloud privato è un'infrastruttura utilizzata esclusivamente da un'organizzazione; le sue risorse non sono condivise, ma isolate e dedicate. Un Cloud privato ospitato fornisce alle aziende i mezzi necessari per aumentare la flessibilità e l'efficacia operativa, mitigando nel contempo i rischi più comuni associati ai Cloud aziendali. In un ambiente di Cloud privato ospitato, una parte del controllo e della responsabilità della sicurezza viene affidata a un provider di servizi di fiducia. Alla luce di ciò, per affrontare queste sfide è essenziale scegliere un fornitore affidabile, con una solida esperienza nella sicurezza.

OVHcloud è un provider globale e il leader europeo del Cloud che gestisce 400.000 server nei 32 datacenter in 4 continenti. Da 20 anni il Gruppo si avvale di un modello integrato che fornisce il pieno controllo della catena del valore, dalla progettazione dei propri server alla gestione dei datacenter fino all'orchestrazione della rete proprietaria in fibra ottica. Questo approccio unico permette a OVHcloud di coprire, in modo indipendente, l'intero spettro di casi d'uso per i 1,6 milioni di clienti in oltre 140 Paesi. OVHcloud offre ai clienti soluzioni di ultima generazione che combinano prestazioni elevate, prezzi prevedibili e piena sovranità dei dati per sostenerne la crescita incondizionata.