Sei modi in cui il cloud computing supporta la sicurezza

Per le aziende, adottare il cloud computing significa dover scegliere tra i costi accessibili, la scalabilità e la convenienza di un ambiente cloud e la comodità di mantenere i dati e le applicazioni al sicuro in hosting sui propri server. Ma le soluzioni on premise sono davvero più sicure del cloud computing? Molti esperti credono di no. I sei aspetti illustrati in questa checklist dimostrano perché puoi passare al cloud computing in tutta tranquillità.

1 La sicurezza costa

La sicurezza richiede investimenti di denaro significativi. In questo senso è bene chiedersi: quanto può permettersi di spendere la mia azienda? Integrare la sicurezza necessaria nel datacenter on premise ha costi proibitivi, soprattutto per le piccole e medie imprese. Raggiungere un livello di sicurezza paragonabile a quello che gli hyperscaler offrono ai propri clienti è inverosimile.

2 La sicurezza richiede personale numeroso

Allo stesso modo, la sicurezza richiede la presenza di più personale. I provider cloud su larga scala dispongono di team di sicurezza attivi 24 ore su 24, 7 giorni su 7, e di un centro operativo completo dedicato al monitoraggio continuo dell'infrastruttura IT e dell'hardware fisico. Ad esempio, la sicurezza di Microsoft Azure è affidata a un team di oltre 3.500 esperti di cybersecurity. La maggior parte delle aziende non ha a disposizione personale a sufficienza per garantire lo stesso livello di sicurezza degli hyperscaler.

3 I provider cloud si intendono di sicurezza

Garantire la sicurezza è importante, ma non è compito tuo. Se per te è solo una delle tante preoccupazioni, per i provider cloud è una priorità assoluta. Per restare competitivi sul mercato, i provider cloud devono infatti garantire ai clienti il livello di sicurezza più alto possibile. Ad esempio, Google Cloud offre un'infrastruttura secure by design, dotata di protezioni integrate e cifratura per impostazione predefinita.[1]

Microsoft Azure individua le minacce "tramite l'analisi di un numero elevato di risorse, tra cui 18 miliardi di pagine web di Bing, 400 miliardi di email, 1 miliardo di aggiornamenti di dispositivi Windows e 450 miliardi di autenticazioni mensili usando il machine learning, le analisi comportamentali e l'intelligenza basata sulle applicazioni offerti dal Microsoft Intelligent Security Graph".[2]

I provider cloud devono anche essere conformi agli standard più elevati, tra cui certificazioni indipendenti e riconosciute a livello internazionale, ma anche audit di persone, processi e tecnologie dedicati alla sicurezza tramite una serie di programmi rigorosi. Ad esempio, Amazon Web Services (AWS) raggiunge regolarmente la convalida di terze parti per migliaia di requisiti di conformità globali. Molte aziende non dispongono del tempo, delle risorse o del budget necessari per raggiungere un livello di sicurezza paragonabile.[3]

1 *"Trust and security." Google, consultato il 29 aprile 2022.*

2 *"Rafforza la tua postura di sicurezza con Azure." Azure, consultato il 29 aprile 2022.*

3 *"Sicurezza del cloud AWS." Amazon, consultato il 29 aprile 2022.*

4 Strumenti di sicurezza avanzati

I provider cloud impiegano diversi strumenti di sicurezza avanzati per proteggere i dati e le applicazioni dei clienti. AWS offre il controllo a grana fine degli accessi e dell'identità, il monitoraggio continuo, il rilevamento delle minacce, la protezione delle applicazioni e delle reti, diversi livelli di cifratura, l'automazione della risposta agli imprevisti e del ripristino, e tanto altro. Gli hyperscaler danno accesso a centinaia di soluzioni di sicurezza aggiuntive, disponibili nei marketplace dei partner. Avere a disposizione questo ampio set di strumenti avanzati nella propria rete e nel datacenter è virtualmente impossibile. I costi, il personale, il tempo e l'impegno richiesti sono troppo elevati per un'azienda che non è specializzata in sicurezza.

5 Segmentazione della rete

Un vantaggio di sicurezza intrinseco degli ambienti cloud è la segmentazione dalle workstation degli utenti. Spesso gli attacchi informatici vengono perpetrati nei confronti degli utenti specifici di un sistema tramite email e siti web. In questi casi, la violazione del sistema avviene attraverso le workstation degli utenti. In un ambiente cloud, tuttavia, la connettività delle workstation è limitata alle operazioni che gli utenti devono svolgere. Le workstation non hanno accesso diretto alla rete aziendale, perciò anche se vengono compromesse, i malintenzionati non possono raggiungere le applicazioni e i dati dell'organizzazione.

6 Sicurezza fisica

La sicurezza fisica è un fattore ancora rilevante. Chi ha accesso fisico diretto all'hardware rappresenta un potenziale rischio di sicurezza. Tuttavia, se i dati e le applicazioni si trovano in un ambiente cloud, gli impiegati malintenzionati e coloro che potrebbero causare danni accidentali lavorando in loco non hanno facile accesso alle risorse. Individuare i dati in un ambiente cloud diventa molto più complicato.

Inoltre, gli hyperscaler dispongono delle risorse necessarie per evitare il furto fisico dei dati, compresi addetti alla sicurezza, gabbie per server chiuse a chiave e altri controlli di sicurezza fisici all'avanguardia che molte aziende non hanno.

Scopri di più

Leggi la panoramica "I servizi cloud a supporto degli sviluppatori" per scoprire in che modo i Red Hat® Cloud Services possono aiutare le organizzazioni nella transizione verso le applicazioni cloud native.

Italia
it.redhat.com
italy@redhat.com

Europa, Medio Oriente, e Africa (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com
#F31540_0522