Gestire l’accesso al cloud è una priorità

Mag 29, 2019 Marco Schiaffino Approfondimenti, Gestione dati, Prodotto, Scenario, Tecnologia 0

La migrazione di dati e servizi verso “la nuvola” è inarrestabile. Akamai: “serve avere un controllo capillare degli accessi in ogni situazione”.

Quando è cominciata la sbornia della cloud, nessuno avrebbe mai pensato che accanto agli annunciati vantaggi si sarebbero presentate anche così tante problematiche, soprattutto in ambito security.

Negli ultimi mesi, però, abbiamo scoperto a nostre spese che la flessibilità e dinamicità garantita dalla “nuvola” ha un rovescio della medaglia che non possiamo ignorare: apre la strada ad abusi e a un aumento esponenziale della superficie di attacco.

Nel dettaglio, l’accesso a dati e servizi attraverso la cloud pone prepotentemente il problema di chi e come può accedervi. Un tema, quello della verifica dell’identità degli utenti, che in questo ambito sembra ancora essere sottovalutato da molte aziende.

Chi non lo sottovaluta sono le società di sicurezza. **Akamai**, per esempio, ha fatto della sua **Identity Cloud** uno dei punti cardinali della sua attività.

“Gli odierni consumatori nativi digitali si aspettano interazioni eccellenti e sicure, in grado di fornire online experience personalizzate, proteggendo la privacy delle preferenze e dei dati personali” spiegano dalle parti di

Akamai.

Ma di cosa stiamo parlando esattamente? Le soluzioni di nuova generazione, come Identity Cloud, puntano in primo luogo a superare la vecchia logica dell'accesso attraverso sistemi basati esclusivamente su credenziali del tipo "username e password". E lo fanno attraverso la formula del **IDaaS (Identity-as-a-Service)**, erogata dalla società.

Un sistema che permette di utilizzare, per esempio, **sistemi automatizzati per l'identificazione della creazione di account fraudolenti** e protocolli sicuri per l'autenticazione attraverso l'utilizzo di account "esterni" (per esempio quelli dei social network) che i normali sistemi on premise non offrono.

Soprattutto il tutto avviene attraverso un accesso **SSO (Single Sign-On)**, che rende più semplice il tutto sul lato utente. "Con l'accesso SSO, i clienti possono effettuare l'accesso una sola volta per navigare facilmente in tutte le vostre proprietà digitali. L'accesso SSO offre una migliore customer experience e riduce i costi di assistenza e i tassi di abbandono del sito, mantenendo i clienti connessi e coinvolti mentre cambiano agevolmente app e domini" spiegano gli esperti

Akamai.

Dal punto di vista della sicurezza interna, uno degli elementi su cui gli sviluppatori hanno focalizzato la loro attenzione è quella della gestione dell'accesso ai dati e ai servizi. La parola chiave, in questo caso, è "ambito".

In parole povere, il sistema permette di definire in maniera capillare quali siano i dati e i servizi a cui può accedere ogni account, consentendo così di mitigare il danno in caso di una eventuale violazione. Una logica simile a quella della segmentazione, ma decisamente più raffinata e flessibile.

Condividi l'articolo

L'esercito cinese punta ad abbandonare Windows Kaspersky punta sulle startup. Una gara per selezionare i migliori

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/29/gestire-laccesso-al-cloud-e-una-priorita/