Mitigare i rischi di sicurezza nel Cloud pubblico con i Cloud Access Security Brokers (CASB)

Date : 30 gennaio 2017

Introduzione

Il Cloud Computing può ormai considerarsi un paradigma consolidato che le aziende adottano per sfruttare al meglio le capacità della propria infrastruttura IT (adottando un Cloud Privato e/o Ibrido) o, passando completamente ad una modalità di utilizzo a consumo o *pay-per-use*, per ridurre drasticamente i costi di investimento e gestione dell'IT interna (Cloud Pubblico).

L'elevata maturità delle soluzioni offerte, tipicamente in Cloud pubblico, e la diffusione di competenze in ambito Cloud stanno supportando la crescente adozione da parte delle aziende di soluzioni in Cloud dove l'utente può totalmente delegare la gestione del servizio al fornitore avendo così la possibilità di essere maggiormente concentrato sui processi di business (vendita, acquisti, marketing, formazione,...). L'adozione di nuovi servizi esterni all'azienda implica tuttavia una minore capacità di controllo sulle loro effettive performance e stabilità offerte dai fornitori (tipicamente di Cloud pubblico) ed espone l'azienda a potenziali rischi di *cyber* attacchi o perdita di dati. La gestione ed esecuzione dei servizi applicativi e memorizzazione dei dati al di fuori dei perimetri aziendali aumenta, inoltre, il possibile impatto causato da comportamenti non idonei da parte di utenti o amministratori di sistema che possono, volontariamente o involontariamente, portare ad accessi indesiderati, perdita o manipolazione di informazioni sensibili. Questa prospettiva è confermata dall'analisi di Gartner[1] che evidenzia come entro il 2020, il 95% dei incidenti di sicurezza saranno dovuti a responsabilità dirette degli utenti. Per questa ragione, è fondamentale per le aziende dotarsi di sistemi, politiche di sicurezza e processi in grado di mitigare tali rischi.

I Cloud Access Security Brokers

La ricerca accademica e i principali fornitori di tecnologia ICT hanno studiato diverse modalità e approcci per mitigare questi problemi di sicurezza, giungendo alla definizione di un "punto di controllo" che si frappone tra gli utenti e il fornitore Cloud in modo da intervenire nell'applicazione delle politiche di sicurezza aziendale nel momento in cui si accede alle risorse in Cloud. Questo servizio di protezione aggiuntivo è oggi noto con il nome di Cloud Access

Security Broker (CASB) che, malgrado siano oggi ancora poco utilizzati, gli analisti definiscono come futura *best practice* con una previsione di adozione pari all'85% entro il 2020.

I CASB supportano e consolidano molteplici aspetti della gestione della sicurezza aziendale, tra cui:

- la conformità con leggi, norme di settore e standard,
- la corretta gestione della sicurezza dei dati,
- l'identificazione delle attività e la completa integrazione con sistemi aziendali pre-esistenti (es. monitoring, ticketing, LDAP, ecc.).

Per gestire efficacemente la sicurezza dei sistemi e dei dati aziendali i CASB sono in grado di monitorare le policy di sicurezza sia per i dispositivi direttamente collegati alla rete aziendale sia per i dispositivi mobili in dotazione a dipendenti e partner commerciali. I servizi Software as a Service (SaaS), infatti, sono in gran parte utilizzati da dispositivi mobili che possono essere compromessi se rubati o collegati a connessioni internet non sicure (es. Wi-Fi pubblico) causando potenziali impatti alla sicurezza di servizi e dati sensibili.

Figure 1- CASB architettura logica

Benefici forniti dai CASB

I CASB offrono una serie di funzionalità che possono essere raggruppate in quattro principali categorie:

- *Visibilità:* individuazione dei servizi Cloud non direttamente gestiti (*shadow* IT) e creazione di una visione consolidata dei servizi e dei dati utilizzati dagli utenti. Nel prossimo futuro i fornitori di servizi Cloud stanno valutando la possibilità di inserire una classificazione dell'affidabilità dei provider così da facilitarne la scelta anche da parte delle piccole e medie imprese dove il dipartimento IT è spesso carente di competenze specifiche in ambito Cloud security
- *Compliance:* controllo della gestione dei dati secondo le leggi in vigore, norme di settore ed i principali standard internazionali ed identificazione dei rischi relativi a specifici servizi Cloud
- *Sicurezza dei dati:* miglioramento delle policy di sicurezza sui dati per prevenire attività non autorizzate ed applicazione automatica di queste attraverso comandi standard (es. alert, block, quarantine, delete, ecc.) in grado di eliminare i dati salvati in modo non autorizzato dai dispositivi direttamente gestiti dall'azienda (es. notebook, tablet e smartphone aziendali)

- *Protezione dalle minacce:* identificazione di comportamenti anomali degli utenti (*EUBA*[2]) ed identificazione di accessi non autorizzati ad applicazioni e dati sensibili
- *Integrazione Aziendale:* interfacciamento con sistemi aziendali pre-esistenti per garantire la corretta integrazione con gli attuali processi ed evitare impatti sulla customer experience (es. user access management, Ticketing and reporting systems, etc.)

Lo studio di CSA "The Treacherous 12: Cloud Computing Top Threats 2016"[3] aiuta a capire i rischi associati all'adozione di servizi in Cloud pubblico, focalizzando l'attenzione su 12 principali minacce di sicurezza che devono essere gestite per garantire la stabilità dei sistemi e la corretta gestione dei relativi dati.

Ben nove delle dodici minacce individuate dalla ricerca possono essere mitigate e costantemente monitorate grazie alla adozione di sistemi CASB:

- **Violazione dei dati (Data breach):** il CASB permette la rilevazione di violazione dei dati, monitorando gli utenti privilegiati, le politiche di sicurezza per la cifratura dei dati e lo spostamento di informazioni sensibili impedendo o limitando l'impatto provocato da comportamenti anomali o accessi non autorizzati.
- **Sicurezza delle interfacce di programmazione di un'applicazione o API**[4] **(Insecure APIs):** il CASB è in grado rilevare chiamate API anomale ed allerta l'utente e l'amministratore del servizio assegnando un punteggio di rischio alle API esterne ed alle applicazioni basate su tali attività.
- **Sicurezza delle credenziali di accesso (Weak ID, Credential and Access Management):** il CABS aiuta a migliorare la sicurezza nell'utilizzo delle credenziali di accesso, monitorando le politiche di sicurezza relative alla scadenza delle password e rilevando eventuali schemi di accesso degli utenti e la conformità dell'utilizzo delle chiavi di crittografia.
- **Vulnerabilità delle applicazioni e sistemi (System and Application Vulnerability):** il CASB supporta la sicurezza dei sistemi attraverso il monitoraggio continuo dei cambiamenti delle configurazioni o si verifichino modifiche nel modello di accesso.
- **Furto delle credenziali utente per compiere azioni illecite (Account Hijacking**[5]**):** mediante il monitoraggio degli utenti, degli account privilegiati, degli account di servizio e delle chiavi per l'accesso alle API, il CABS può rilevare minacce di *account hijacking* grazie a tecniche di machine learning ed analisi del comportamento.
- **Compromissione dell'infrastruttura ICT del fornitore Cloud (Shared Technology Issues):** Il CASB riduce i rischi di compromissione dei servizi utilizzati monitorando le risorse infrastrutturali ed applicative, spesso condivise, ed assicurando la corretta segregazione delle stesse.
- **Abuso dei servizi Cloud (Abuse & Nefarious Use of Cloud Services):** il CASB aiuta a ridurre i rischi di abuso dei servizi in Cloud, monitorando i carichi di lavoro a livello Infrastructure as a Service (IaaS) ed i modelli di accesso nei servizi SaaS per rilevare esecuzioni anormale di istanze di calcolo e modelli di accesso utente anomali.
- **Attacchi mirati e continuativi (Advanced Persistent Threats):** Il CASB è in grado di rilevare anomalie di dati in entrata ed in uscita (*data exfiltration***[6]**), aiutando a scoprire se una rete è stata oggetto di un attacco APT bloccandone il punto di accesso
- **Utenti o fornitori infedeli (Malicious Insider)**: Il CASB può monitorare l'eccessivo uso

dei privilegi utenti che deviano dalle linee guida di conformità rilevando attività maliziose di utenti attraverso strumenti di analisi del comportamento utente (UEBA - User Behavior Analytics)

Principali modelli di erogazione di un servizio CASB

I servizi CASB si stanno affermando sostanzialmente attraverso i modelli di erogazione del servizio *Proxy-based* e *API-based*. Le aziende devono quindi prestare attenzione alla architettura del CASB e ai servizi da esso supportati per garantire la massima copertura possibile. Le architetture Proxy e API sono molto diverse tra loro ed assicurano un diverso livello di protezione.

Modello Proxy-based

Il modello *Proxy-based* gestisce la sicurezza di utenti e dispositivi conosciuti attraverso un singolo punto di controllo o proxy dove l'intero traffico viene convogliato e controllato ed in cui vengono applicate le diverse policy di sicurezza in tempo reale. Utilizzare un singolo punto di controllo introduce però il rischio di impatti diretti sulle performance della rete (in particolare la latenza, ovvero i tempi di risposta del servizio) che può direttamente riflettersi sulle prestazioni generali del servizio cloud utilizzato, compromettendo la corretta fruibilità dello stesso (*user experience)*. Inoltre, il proxy richiede particolari configurazioni sui diversi dispositivi di accesso (es. notebook, tablet, smartphone, ecc.) e permette quindi il controllo dei soli dispositivi ed utenti conosciuti e direttamente gestiti dalla azienda.

Figure 2 - CASB proxy based

Modello API-based

Il modello *API-based* può considerarsi una soluzione "*out-of-band*"[7] che non segue lo stesso percorso dei dati gestiti dai servizi Cloud. L'integrazione diretta con i servizi Cloud non impatta le performance della network ed è in grado di gestire i collegamenti eseguiti da dispositivi ed utenti conosciuti e non conosciuti. A supporto dell'adozione di tale modello, Cloud Security

Alliance (CSA) sta lavorando allo sviluppo di un set standard di API in grado di garantire la corretta compatibilità tra CASB e i principali servizi Cloud.

Figure 3 - CASB APIs based

Nel breve futuro, gli analisti di mercato ed esperti Cloud prevedono l’adozione di un approccio multimodale in modo da beneficiare delle diverse funzionalità offerte e diversificare la gestione della sicurezza tra le tipologie di utenti.

Di seguito viene riportato un breve confronto tra le modalità Proxy-based e API-based precedentemente descritte:

In grado di scansionare archivi Cloud esistentiNessuna capacità di scansionare archivi Cloud esistenti

Visibilità	Tutti i tipi di traffico	Solo su utenti e i dispositivi gestiti
Compliance	Supporta la certificazione di HIPAA, PCI DSS e di altri mandati di data governance	Supporta la compliance solo per gli utenti gestiti e i dati in transito

Modelli Cloud	Assicura tutti i modelli di delivery (IaaS, PaaS, SaaS)	Assicura solo SaaS
Controllo accessi	Integrazione con servizi di Identity as a service (IDaaS)	Supporto incorporato nel proxy
Data loss prevention	In grado di scansionare archivi Cloud esistenti	Nessuna capacità di scansionare archivi Cloud esistenti
Scalabilità	Nessun particolare limite di scalabilità	Capacità del proxy da gestire per evitare latenza
Scansione	Identifica l'utilizzo di applicazioni autorizzate e non	Identifica l'utilizzo di applicazioni autorizzate e non

Conclusioni

Le aziende che vorranno far leva sui servizi in Public Cloud per applicazioni *mission-critical* e dati sensibili dovranno rivedere i requisiti di governo delle sicurezza dei dati sotto una diversa lente. L'aumento della maturità delle soluzioni in Cloud pubblico e la massiccia spinta verso la mobilità del lavoro (es. BYOD, smart working, ecc.) introducono una serie di variabile scarsamente controllabili con gli attuali sistemi in dotazione alle aziende. L'adozione di sistemi CASB come punti di controllo della sicurezza dei servizi Cloud aumenta la visibilità sugli accessi e le transazioni effettuati a sistemi, applicazioni e dati garantendo un diretto controllo sulla policy di sicurezza aziendale. La combinazione delle funzioni dei CASB, strettamente integrate con il fornitore Cloud e le policy di sicurezza aziendale, possono indirizzare i principali requisiti di governo della sicurezza dei servizi mitigando i rischi intrinsechi alla migrazione nel Cloud pubblico.

Note

[1] Gartner Press Release, "*Gartner Reveals Top Predictions for IT Organizations and Users for 2016 and Beyond*" October 6, 2015, http://www.gartner.com/newsroom/id/3143718

[2] UEBA - User Behavior Analytics

[3] https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/

[4] Application Programming Interface

[5] https://digitalguardian.com/blog/what-cloud-account-hijacking

[6] https://digitalguardian.com/blog/what-data-exfiltration

[7] https://en.wikipedia.org/wiki/Out-of-band_management

A cura di: **Nicola Sfondrini** e **Domenico Catalano**