

Cloud computing forensics: peculiarità e indicazioni metodologiche

Il Cloud computing è il principale modello di deployment dei servizi online, applicazioni, risorse e dati; è adottato da tutte le organizzazioni, indipendentemente dal settore, dalle dimensioni o dalle esigenze di calcolo e/o di storage. Di conseguenza, è cresciuto il contenzioso avente ad oggetto il cloud, ovvero i servizi e i dati in cloud. La specificità, la complessità e l'eterogeneità dell'ambiente cloud, rispetto agli ambiti on-premise, richiedono un approccio e un metodo di conduzione delle indagini digitali ad hoc. In questo articolo provo a evidenziare le peculiarità tecniche e descrivere una metodologia conforme agli standard di settore e agli obiettivi prescritti dalle norme.

Introduzione

Il Cloud computing è il principale modello di deployment dei servizi online, applicazioni, risorse e dati; è adottato da tutte le organizzazioni, indipendentemente dal settore, dalle dimensioni o dalle esigenze di calcolo e/o di storage. Di conseguenza, è cresciuto il contenzioso avente ad oggetto il cloud, ovvero i servizi e i dati in cloud. Le principali controversie, fin qui registrate, hanno riguardato:

- **i termini e/o le condizioni di servizio.** Spesso i contratti di fornitura dei servizi in cloud sono generici e lacunosi, in particolar modo nella definizione dei service-level agreement (SLA), oppure non sono conformi alle normative e regolamenti vigenti, per esempio in tema di cybersecurity, continuità operativa e privacy, e ciò genera il contenzioso in fase

di esecuzione del contratto;

- **la violazione alla sicurezza e/o alla privacy dei dati o dei servizi.** Il cloud computing è indubbiamente più esposto a questa tipologia di minacce, per cui è necessario conoscere le tecniche di indagine specifiche per le violazioni che hanno compromesso la confidenzialità, l'integrità e la disponibilità dei dati o dei servizi in cloud;
- **lo sfruttamento della capacità di calcolo e/o memorizzazione.** La disponibilità elevata di risorse offerte dal cloud computing è divenuto un obiettivo dei criminali informatici per perpetrare attività illecite o sfruttare la capacità di calcolo a carico di altri.

La specificità, la complessità e l'eterogeneità dell'ambiente cloud, rispetto agli ambiti on-premise, richiedono un approccio e un metodo di conduzione delle indagini digitali ad hoc. In questo articolo provo a evidenziare le peculiarità tecniche e descrivere una metodologia conforme agli standard di settore e agli obiettivi prescritti dalle norme vigenti.

Cloud computing

Definizione e proprietà funzionali

Il termine cloud computing indica una modalità di erogazione di servizi ICT offerti da alcuni operatori (provider) a una moltitudine di utenti (user) in modalità on demand e pay-per-use. Questi servizi sono erogati mediante infrastrutture hardware e software di proprietà dei provider o della stessa organizzazione senza una gestione attiva diretta da parte dell'utente; questi ultimi accedono attraverso le tecnologie e i protocolli di rete. Tipicamente un sistema cloud si compone di uno o più data center organizzati secondo un'architettura distribuita. Il principio cardine del cloud computing è la virtualizzazione: tutte le risorse di elaborazione, memorizzazione e trasmissione sono virtuali, ovvero ottenute

sfruttando tecniche di emulazione implementate su risorse fisiche. Un tipico sistema cloud utilizza i gestori delle risorse (Hypervisor per la distribuzione di macchine virtuali, Container Engine per la distribuzione dei servizi o microservizi), che hanno il compito di amministrare le risorse fisiche dell'infrastruttura, allocandole dinamicamente alle diverse risorse virtualizzate (macchine virtuali o container) che condividono tale infrastruttura.

I principali vantaggi del cloud computing non si limitano solo alla riduzione dei tempi e dei costi, ma anche all'agilità e alla scalabilità. In particolare, i sistemi cloud sono caratterizzati da proprietà funzionali con un impatto significativo sulle investigazioni digitali:

- **Distribuzione geografica delle risorse:** i data center che ospitano l'hardware di un sistema cloud sono organizzati secondo un'architettura distribuita, ovvero sono partizionate su un set di siti indipendenti, ubicati a distanza tra di loro. Di conseguenza, le risorse e i dati relativi ad uno specifico utente possono essere ubicati su una pluralità di dispositivi diversi, per cui può risultare complesso individuare l'ubicazione di tutti i dati riconducibili a tale utente, oltre a rappresentare un grosso problema in termini di giurisdizione territoriale.
- **Elasticità, scalabilità e flessibilità:** l'utente di un servizio cloud può variare dinamicamente la quantità e la tipologia di risorse allocate. Pertanto, le risorse utilizzate da un utente in uno specifico arco temporale possono non essere più nella disponibilità di tale utente in un momento successivo e rischia di creare false istanze.
- **Gestione dinamica delle risorse:** i sistemi cloud impiegano politiche di gestione delle risorse in cui quelle virtualizzate possono essere fatte migrare tra le varie risorse fisiche. Per cui può divenire ancora più

complesso individuare tutti i dati e le risorse riconducibili ad un determinato utente, nonché ricostruire la sequenza di risorse fisiche su cui sono stati allocati.

- **Multi-tenancy:** in un sistema cloud coesistono servizi riconducibili a soggetti diversi (tenant) che condividono le stesse risorse fisiche. La multi-tenancy produce due effetti: consente di ottenere adeguati livelli di privatezza dei dati grazie all'adozione di meccanismi crittografici; rende difficile risalire alla paternità degli artefatti presenti su una determinata risorsa fisica.
- **Trasferimento della responsabilità:** gli utenti di un sistema cloud non hanno la possibilità di esercitare un livello di controllo completo sulle proprie risorse virtualizzate e hanno difficoltà a comprendere come vengono gestiti i propri dati. Il livello di controllo dipende dalla modalità di erogazione del servizio. Più la risorsa virtuale è profonda, più l'utente disporrà di controlli sulle risorse e viceversa.

La natura distribuita dei sistemi cloud, la condivisione tra utenti diversi, l'uso di tecnologie di virtualizzazione, l'adozione di meccanismi di replicazione e migrazione di risorse e dati, una stratificazione di responsabilità dovuta alla presenza di componenti forniti da soggetti diversi, pongono svariate criticità che il forenser deve essere in grado di comprendere e, opportunamente, acquisire e gestire, al fine di preservare le proprietà di genuinità, immodificabilità e verificabilità della potenziale evidenza.

Tipologia di fruizione dei servizi

Tipicamente i servizi in cloud sono erogati in una delle modalità di seguito indicate, talvolta combinate tra loro, ovvero:

- **On-premise:** è il modello in cui l'hardware, le

applicazioni, la connettività e tutti gli altri strumenti necessari, per esempio per la sicurezza o la scalabilità, sono di proprietà; pertanto, la gestione e la responsabilità ricade sulla stessa organizzazione;

- **Infrastructure-as-a-Service (IaaS):** è il modello in cui il provider offre l'accesso on-demand a server fisici e virtuali, storage e reti in hosting sul cloud, l'infrastruttura IT di back-end per eseguire le applicazioni e i carichi di lavoro sul cloud, denominato Hypervisor. Esempi di servizi erogati in IaaS: Amazon Web Services (AWS), Google Cloud Platform (GCP);
- **Container as a Service (CaaS):** è un modello in cui il provider consente l'accesso on-demand ad ambienti in cui sono offerti i servizi di base, denominati Container Engine, per eseguire le applicazioni (Container). Esempi di servizi erogati in CaaS: Docker e Google Kubernetes Engine (GKE);
- **Platform-as-a-Service (PaaS):** è un modello in cui il provider consente l'accesso on-demand a una piattaforma di hosting su cloud, pronta all'uso e completa, per lo sviluppo, l'esecuzione, la manutenzione e la gestione di applicazioni, denominati Servless runtime. Esempi di servizi erogati in PaaS: Heroku, Google App Engine, Microsoft Azure App Service;
- **Function as a Service (FaaS):** è un modello in cui il provider consente l'accesso on-demand per creare ed eseguire il deployment di una piccola porzione di codice o di una funzione che esegue un'attività specifica (per esempio un Microservizio). Quando viene eseguita una funzione, il cloud provider aggiunge scalabilità secondo necessità. Esempi di servizi erogati in FaaS: AWS Lambda, Azure Functions, Google Cloud Functions;
- **Software-as-a-Service (SaaS):** è un servizio che consente l'accesso on-demand a software applicativo in hosting sul cloud e pronto all'uso. Esempi di servizi erogati in SaaS: Salesforce, Google Workspace, Microsoft 365 e SAP Business ByDesign.

Nell'ambito delle investigazioni digitali, la comprensione della tipologia di erogazione di servizio cloud riveste un ruolo fondamentale perché aiuta a comprendere l'oggetto dell'indagine, il tipo di evidenze da acquisire, gli strumenti e la metodologia da utilizzare; inoltre, consente di tracciare il confine tra le informazioni utente e quelle del provider, individuare le responsabilità in termini contrattuali e, in caso di incidente, la corretta attribuzione dell'eventuale condotta colposa e/o dolosa. L'immagine sottostante raffigura sinteticamente l'ambito di controllo e la responsabilità nelle diverse configurazioni di cloud.



Modelli di deployment – Livelli di Responsabilità (Fonte: Google cloud)

In informatica forense è fondamentale comprendere il concetto 'As a service'. Esso si riferisce al modo in cui gli asset IT vengono utilizzati e alla differenza sostanziale tra cloud computing e IT tradizionale. Nell'IT tradizionale, un'organizzazione usa gli asset IT, hardware, software di sistema, strumenti di sviluppo, tools per la sicurezza, applicazioni, che acquista, installa, gestisce e di cui effettua la manutenzione nel proprio data center on-premise. Nel cloud computing, il provider di servizi cloud è il proprietario e il responsabile della gestione e della manutenzione degli asset; il cliente utilizza tali asset tramite una connessione Internet e paga in base a un abbonamento o con la modalità PAYG (pay-as-you-go – pagamento a consumo). Inoltre, nella pratica, i servizi di cui fruisce un utente del cloud sono forniti da diverse entità; pertanto, è fondamentale mappare i vari strati e le responsabilità al fine di identificare le evidenze e attribuire la corretta paternità.

Modelli di deployment dei sistemi

Un modello di deployment specifica come è realmente

implementata un'architettura software su un'infrastruttura fisica, per esempio tramite l'allocazione di più istanze software su diverse componenti dell'infrastruttura fisica; pertanto, è fondamentale comprenderla prima di avviare un'indagine digitale. In un determinato sistema possono coesistere diversi modelli di deployment, che si possono differenziare tra loro per l'obiettivo che cercano di perseguire: prestazione del sistema, disponibilità dei servizi erogati, sicurezza e/o privacy dei dati, costo. Molti obiettivi sono divergenti, per cui non è possibile che siano tutti massimizzati.

In ambito cloud sono stati sviluppati diversi modelli di deployment, ognuno progettato per massimizzare determinato obiettivi, tra cui:

- **cloud pubblico:** i provider offrono le risorse ad una pluralità di utenti, nessuno dei quali ha l'accesso esclusivo alle risorse. Il cloud pubblico consente all'utente di ottenere un vantaggio economico, per quanto riguarda i costi di avvio e di gestione, e di sgravarsi dalla responsabilità del rischio operativo inerente all'infrastruttura IT. Tuttavia, non consente agli utenti di esercitare un controllo completo sulle risorse utilizzate e, pertanto, risulta poco adatto agli scenari business-oriented, in cui il controllo è essenziale;
- **cloud privato:** è concepito per l'utilizzo esclusivo da parte di un solo soggetto utente. Di conseguenza, offre il miglior grado di controllo su prestazioni, affidabilità e sicurezza, a discapito dei costi operativi;
- **cloud ibrido:** è una combinazione tra cloud privato e pubblico e cerca di coniugare i vantaggi di entrambe, evitando al contempo gli svantaggi. In un cloud ibrido parte dell'infrastruttura è utilizzata esclusivamente da un unico soggetto, mentre la parte restante è messa a

disposizione di altri. L'unica criticità di questa soluzione consiste nel prevedere dei meccanismi e delle politiche in grado di mantenere separate la partizione pubblica da quella privata;

- **multi-cloud:** è una combinazione di servizi cloud di due o più fornitori compatibili con specifici requisiti e con il carico di lavoro richiesto. In altri termini, il multi-cloud è una tecnologia cloud ibrida agile e flessibile che utilizza molti servizi di infrastruttura cloud pubblica per ottimizzare le performance, i costi di gestione e la continuità operativa.



Modelli di deployment – Tradizionale, pubblico, privato, ibrido, multi cloud



Questo articolo è stato estratto dal white paper “Cloud Computing Forensics: Peculiarità e Indicazioni Metodologiche” disponibile in maniera libera e gratuita al seguente link: <https://www.ictsecuritymagazine.com/pubblicazioni/cloud-computing-forensics-peculiarita-e-indicazioni-metodologiche/>

Articolo a cura di **Vincenzo Calabrò**

Profilo Autore



Referente Informatico e Funzionario alla Sicurezza CIS (Ministero dell'Interno).

È laureato in Ingegneria Informatica ed in Sicurezza Informatica presso le Università di Roma La Sapienza e di Milano. Ha, altresì, indirizzato la sua formazione nei settori della Cyber Security e Digital Forensics conseguendo i Masters in Data Protection e Data Governance, IT Risk Management e Sicurezza Informatica ed Investigazioni Digitali, oltre al CERT Certification in Digital Forensics rilasciato da Carnegie Mellon University, all'European Certificate on Cybercrime and E-Evidence (ECCE) rilasciato dall'European Commission's

Directorate General Justice, Freedom and Security.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/cloud-computing-forensics-peculiarita-e-indicazioni-metodologiche/>