CLOUD COMPUTING FORENSICS:

PECULIARITÀ E INDICAZIONI METODOLOGICHE

Vincenzo Calabrò
Funzionario alla Sicurezza CIS (Ministero dell'Interno)
e Digital Forensics Analyst

WHITEPAPER 07/2024

ICT Security MAGAZINE

INDICE

ICT Security MAGAZINE

CYBER CRIME CONFERENCE

17-18 APRILE 2024

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
12ª Edizione della Cyber Crime Conference

ABOUT THE AUTHOR

Vincenzo Calabrò

Funzionario alla Sicurezza CIS (Ministero dell'Interno) e Digital Forensics Analyst

È laureato in Ingegneria Informatica ed in Sicurezza Informatica presso le Università di Roma La Sapienza e di Milano. Ha indirizzato la sua formazione nei settori della Cyber Security e Digital Forensics ottenendo i diplomi di perfezionamento in Data Protection e Data Governance; Criminalità Informatica e Investigazioni Digitali e Big Data, Artificial Intelligence.

Ha, altresì, conseguito l'Advanced Cybersecurity Graduate Certificate alla School of Engineering della Stanford University; Professional Certificates in Information Security; Incident Response Process; Digital Forensics e Cybersecurity Engineering and Software Assurance presso il Software Engineering Institute della Carnegie Mellon University.

Dal 1992 è nei ruoli del Ministero dell'Interno ove ricopre lincarico di Funzionario alla Sicurezza CIS. In tale veste contribuisce alla valutazione dei rischi cyber, all'implementazione delle misure di sicurezza e la risoluzione di incidenti informatici. Inoltre, offre consulenza tecnica nel campo della Digital Forensics per l'Autorità giudiziaria, la Polizia giudiziaria e gli Studi legali.

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 contezioso 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:

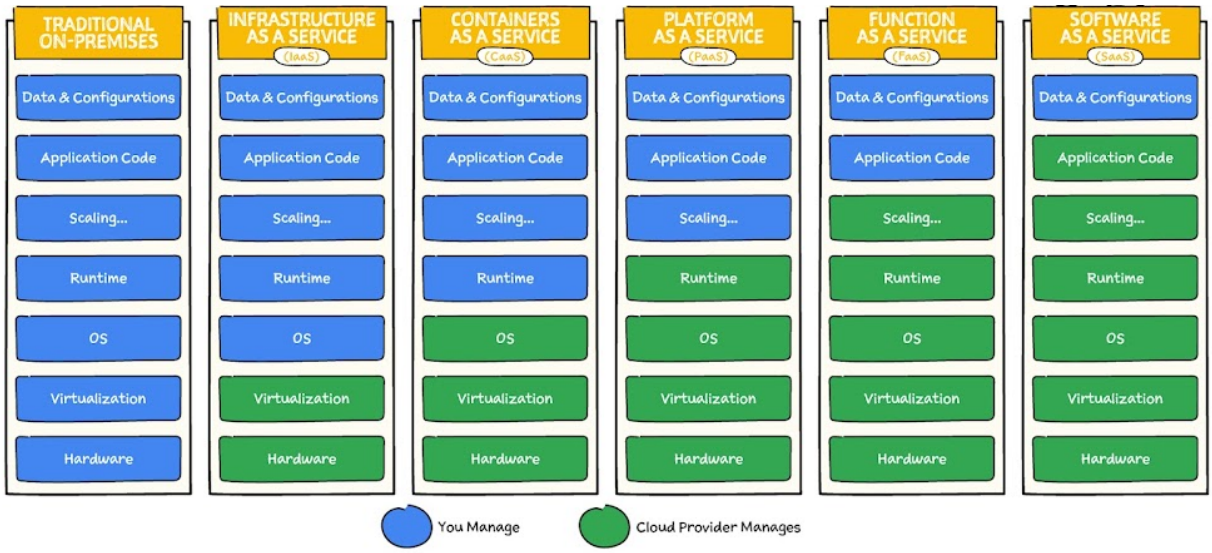
- **On-premise**: è il modello in cui l'hardware, le applicazioni, la connettività e tutti gli altri strumenti necessari, per esempio per la sicurezza o la scalabilità, sono di proprietà; pertanto, la gestione e la responsabilità ricade sulla stessa organizzazione;
- **Infrastructure-as-a-Service (IaaS)**: 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 successiva raffigura sinteticamente l'ambito di controllo e la responsabilità nelle diverse configurazioni di 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 – Livelli di Responsabilità (Fonte: Google cloud)

Modelli di deployment dei sistemi

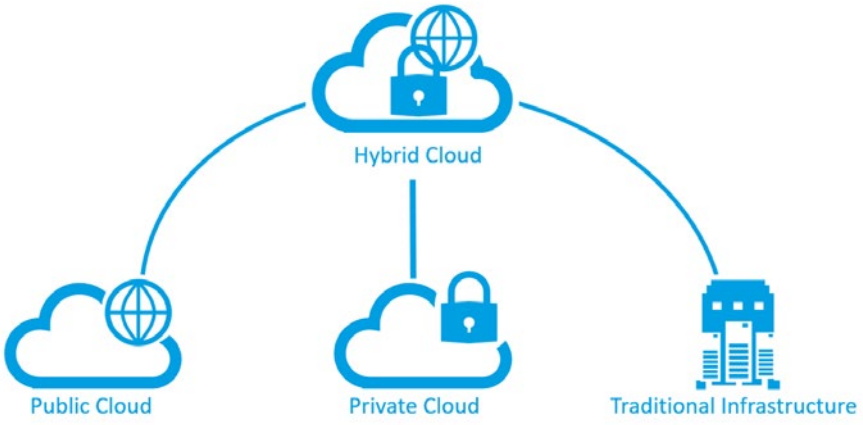
Un modello di deployment specifica come è realmente implementata un'architettura software su un'infrastruttura fisica, per esempio tramite l'allocazione di più istanze software su diverse componenti dell'infrastruttura fisica; pertanto, è fondamentale comprenderla prima di avviare un'indagine digitale. 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 privatezza 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

Elementi di data security e protection

Il cambio di paradigma del cloud computing elimina la dipendenza dai server locali, consente la fruizione delle applicazioni senza soluzione di continuità e offre un'elevata disponibilità di capacità di calcolo e memorizzazione. Inoltre, offre scalabilità, flessibilità ed economicità. Di conseguenza, la sicurezza del cloud riveste un ruolo qualificante.

Le statistiche sugli incidenti informatici che riguardano il cloud rilevano che le principali minacce riguardano l'abuso di credenziali, il cryptomining, i ransomware, il data exfiltration e gli attacchi DOS, mentre i punti deboli della sicurezza del cloud sono rappresentati da credenziali d'accesso deboli o con privilegi elevati, errori di configurazione, vulnerabilità del software di terze parti.

Le organizzazioni che affidano i loro servizi essenziali al cloud computing devono pretendere un modello che contempli il controllo degli accessi, l'adozione di tecniche di crittografia e il monitoraggio continuo del traffico di rete. Inoltre, devono verificare che sia presente una policy di accesso robusta, una gestione proattiva delle patch, gli audit di sicurezza, la valutazione delle vulnerabilità, un sistema di rilevamento delle intrusioni e gli strumenti SIEM. In sintesi, una strategia di sicurezza del cloud si fonda sulla fiducia, garantisce la protezione dei dati e il rispetto dei requisiti legali e degli standard settoriali.

I principali elementi per la sicurezza e protezione dei dati nel cloud sono riepilogati di seguito:

1. **Confidenzialità**: l'accesso ai dati è consentito solo agli utenti autorizzati;
2. **Integrità**: i dati devono rimanere integri e nel formato originale;
3. **Disponibilità**: gli utenti autorizzati devono fruire di un accesso affidabile;
4. **Privacy**: i dati privati devono essere protetti dagli accessi non autorizzati;
5. **Data encryption**: garantire la confidenzialità e la privacy tramite la crittografia dei dati;
6. **Identity and access management** (IAM): garantire un accesso sicuro alle risorse cloud attraverso un sistema di gestione dell'autenticazione e delle autorizzazioni;
7. **Information protection**: classificazione e protezione dei dati sensibili;

8. **Shared responsibility model**: identificare il modello di distribuzione della responsabilità tra provider e organizzazione;
9. **Malicious insiders**: mitigare il rischio insider;
10. **Intentional data remanence**: implementare la rimozione sicura dei dati dallo storage;
11. **Business continuity plan**: prevedere strategie di data backup e data recovery;
12. **Data segregation/multi-tenant services**: distribuire più copie di dati su storage diversi;
13. **Data loss prevention** (DLP): implementare politiche contro la perdita o il furto dei dati
14. **Data protection compliance recommendations**: adottare policy per la compliance normativa.

La conduzione di un'indagine digitale deve necessariamente tenere conto di queste proprietà per un duplice motivo: da un lato serve a individuare le criticità o le vulnerabilità di un sistema cloud, dall'altro agevola la ricerca delle evidenze, come vedremo nel seguito.

Aspect	Cloud Security	Cloud Forensics
Focus	Proactive measures and strategies to safeguard data and resources stored in the cloud	Reactive approach, investigating and analyzing incidents, breaches, or unauthorized activities within the cloud after they have occurred.
Key objective	Prevent unauthorized access, data breaches, and potential threats	Investigate incidents, understand their nature and extent, and enhance overall security readiness.
Key components	Cloud security involves network security measures like firewalls, robust data encryption protocols, and access control mechanisms to protect data at rest and in transit, ensuring a secure cloud environment.	Cloud forensics uses specialized tools for digital evidence collection and analysis, including software, data acquisition, and data interpretation, to reconstruct events in security incidents, enabling investigators to reconstruct the sequence of events.
Role in incident response	Cloud security plays a critical role in establishing a robust defense mechanism to prevent security incidents and breaches. It focuses on proactive measures to minimize the likelihood of incidents occurring in the first place.	Cloud forensics is crucial in incident response, identifying the root causes of security incidents, holding responsible parties accountable, and implementing preventive measures. It collects and analyzes digital evidence post-incident.
Typical activities	Implementing security layers, including network security, data encryption	Collecting and analyzing digital evidence, post-incident analysis.
Expertise required	Security professionals, network administrators	Digital forensic analysts, incident responders
Time frame	Ongoing process to maintain security	Typically initiated after a security incident occurs

Confronto tra gli obiettivi della cloud security e della cloud forensics (Fonte: Research on cloud forensics)

Cloud computing forensics

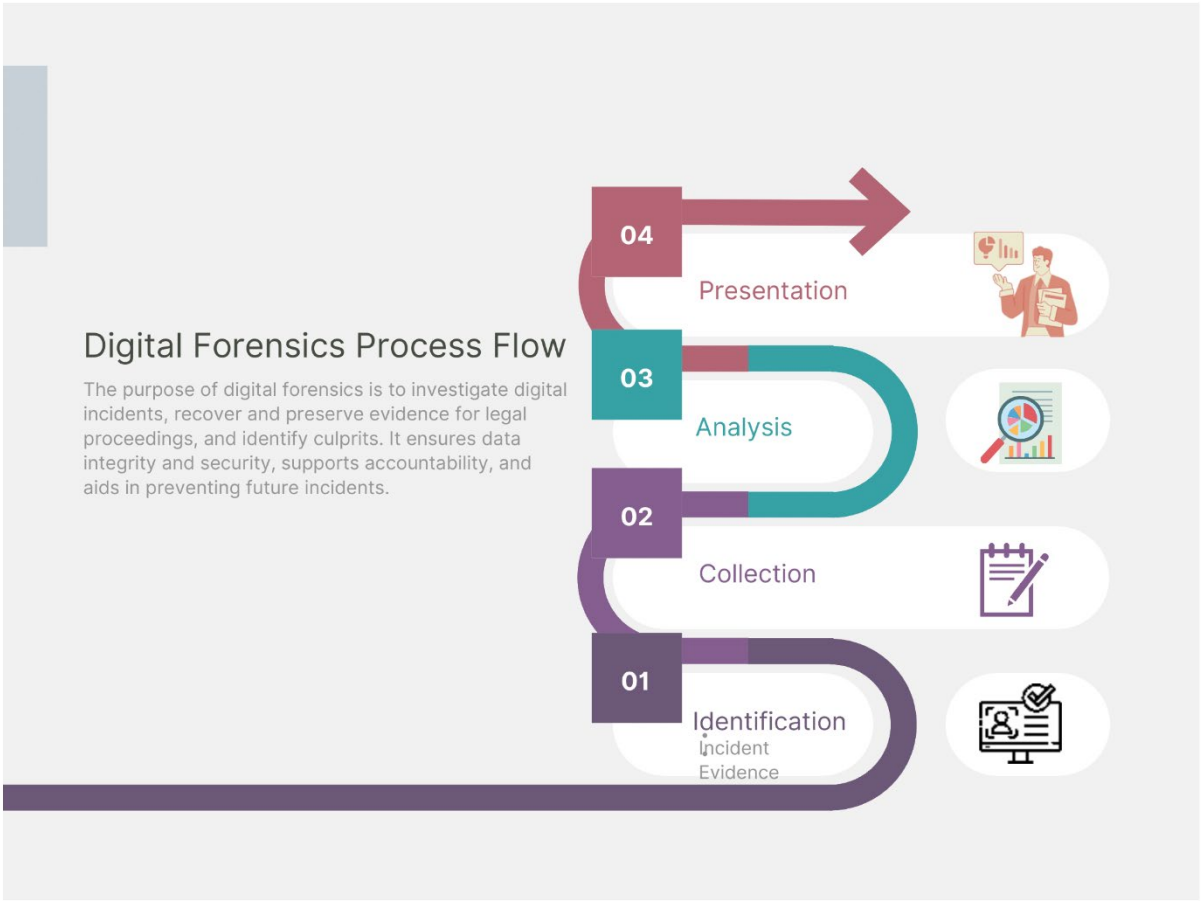
Il cloud computing ha visto il progressivo spostamento di servizi, applicazioni e dati su infrastrutture di elaborazione e storage ubicate presso soggetti terzi rispetto ai loro utenti, gestori o proprietari. Ovviamente, anche i sistemi cloud possono essere oggetto di attività illecite, o essere a loro volta utilizzati per compiere attività di tale genere, per cui è necessario saper effettuare l'analisi forense in questi ambienti, determinare le attività eseguite su di essi o mediante essi, le modalità con cui sono state compiute e il soggetto cui sono riconducibili, ovvero comprendere i diversi livelli di responsabilità nei contenziosi di natura contrattualistica.

La specificità dei sistemi cloud, come la distribuzione e la duplicazione di dati e delle componenti applicative, o anche l'elevato livello di virtualizzazione e segmentazione, richiede specifiche metodologie di analisi forense che rendono difficilmente applicabili, se non inadatte, le metodologie sviluppate per l'analisi dei sistemi on-premise. Queste ultime sono infatti basate sul presupposto che sia possibile accedere, senza restrizioni, ai sistemi e ai dati, ipotesi che non valgono nel cloud computing.

La cloud computing forensics si pone l'obiettivo di sviluppare metodologie e strumenti per l'analisi forense dei sistemi cloud: *«Cloud Computing forensic science is the application of scientific principles, technological practices and derived and proven methods to process past cloud computing events through identification, collection, preservation, examination and reporting of digital data for the purpose of facilitating the reconstruction of these events»*. La letteratura scientifica prevede una sequenza di attività distinte: l'identificazione (identification) delle potenziali fonti di prova digitale, la raccolta (collection) e/o l'acquisizione (acquisition) di tali fonti, la conservazione (preservation), l'analisi (analysis) e, infine, la presentazione (reporting) dei risultati ottenuti. Ogniuna di queste fasi è ben definita dagli standard ISO/IEC 27037:2012 *"Guidelines for identification, collection, acquisition, and preservation of digital evidence"* e ISO/IEC 27042:2015 *"Guidelines for the analysis and interpretation of digital evidence"* (a cui si rimanda per un maggiore approfondimento), ma non indicano le specifiche procedure da adottare per l'attuazione delle varie fasi in un determinato contesto. Pertanto, devono essere definite, tenendo conto delle specificità dei sistemi basati sul cloud computing, affinché sia garantito il rispetto dei requisiti che caratterizzano sia la prova digitale (autenticità e integrità), sia il procedimento e gli strumenti di analisi forense (affidabilità, ripetibilità e giustificabilità dei risultati ottenuti).

Tipicamente un sistema cloud è formato da diversi sottosistemi: **i client** utilizzati per accedere ai servizi, **le risorse virtualizzate** che erogano tali servizi, **le risorse fisiche** utilizzate per la gestione di quelle virtualizzate

e **la rete** che permette l'interconnessione. Mentre per la prima categoria e l'ultima categoria esistono processi consolidati (cd. Computer forensics e Network forensics), per le risorse virtualizzate e gli ambienti che le ospitano occorre sviluppare procedure specifiche. Inoltre, essendo ciascuno di tali sottosistemi diverso dagli altri, richiedono l'applicazione di procedure di analisi ulteriormente personalizzate che potremmo definire "*sartoriali*".



Il processo di cloud digital forensics (Fonte: Research on cloud forensics)

Identification

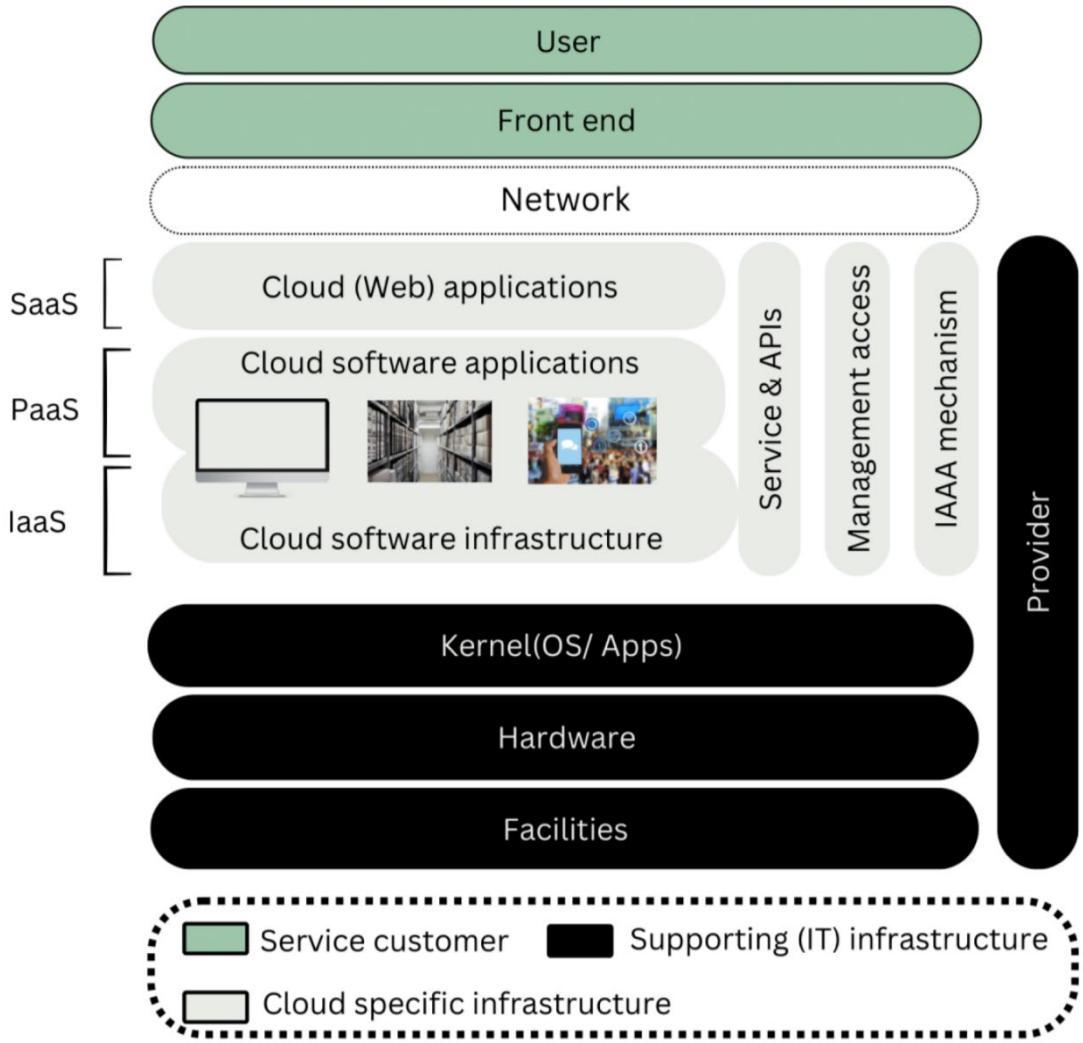
Con il termine Identification si intende *"the process involving the search for, recognition and documentation of potential digital evidence"*, ovvero la ricerca, l'individuazione e la documentazione delle potenziali fonti di prova digitale. Nel contesto del cloud computing consente di individuare le risorse fisiche e virtualizzate, compresi i dati di utilizzo (p.e. i file di log, il controllo degli accessi e le attività degli utenti), potenziali fonti di prova digitale.

L'identificazione richiede:

- **la conoscenza dell'ubicazione delle risorse**: per poterle localizzare all'interno del eco-sistema cloud e identificare il provider,
- **la comprensione delle modalità di accesso e fruizione delle risorse:** per poterle interrogare e acquisire da remoto o on-premise,
- **il formato e la codifica dei dati**: per poterli correttamente decodificare e interpretare ai fini dell'analisi (crittografia);
- inoltre, poiché ogni sottosistema può essere distribuito da un fornitore diverso e con tecnologia diversa, **occorre conoscere gli account con privilegi admin, i servizi oggetto di indagine, la tipologia, i servizi di management, monitoring e security abilitati e la mappatura dei provider**.

L'identificazione non è di semplice attuazione perché occorre fare i conti con una serie di criticità:

- **indeterminazione del posizionamento delle risorse e dei dati**. Il principio cardine su cui si basa il cloud computing è la flessibilità, ovvero la possibilità di replicare e migrare i dati e le risorse virtualizzate sulle varie risorse fisiche facenti parte del sistema cloud. Questo principio diventa un problema in fase di identificazione, ma può essere in parte risolto acquisendo preliminarmente:
  - i log di sistema per rintracciare le risorse all'interno dell'infrastruttura;
  - i tag utilizzati per etichettare i dati e le risorse di un determinato utente;
  - i service level agreements per comprendere gli obblighi contrattuali e le eventuali clausole che incidono sulla localizzazione o l'ubicazione geografica.



Le componenti di un Cloud Computing Service (Fonte: Research on cloud forensics)

- **decentramento delle risorse e dei dati**. Generalmente, le risorse e i dati non sono memorizzati in un'unica risorsa per consentirne un'ottimale disponibilità. Per ricostruire la cronologia delle localizzazioni occorre acquisire i log del framework deputati alla registrazione delle operazioni relative all'utilizzo e alla memorizzazione dei dati.

- **inaccessibilità fisica del sistema**. Le risorse fisiche sono spesso inaccessibili, pertanto è necessario rivolgersi al provider per accedere alle risorse virtuali. I principali provider si stanno attrezzando per queste necessità, offrono soluzioni per l'estrazione della memoria volatile e per la realizzazione di copie del componente virtuale d'interesse.
- **cifratura dei dati**. La necessità di mantenere adeguati livelli di riservatezza dei dati in un ambiente multi-tenancy di solito è soddisfatta mediante l'uso di tecniche di cifratura. Le chiavi di cifratura possono essere gestite dal provider, sottoforma di servizio, oppure direttamente dall'utente.

Per superare alcune delle criticità esposte, è opportuno che il forenser proceda a:

- **acquisire le credenziali o il token degli account con privilegi admin** per accedere all'ambiente cloud dall'esterno;
- **identificare i log del servizio d'interesse e dei servizi cloud correlati;**
- **individuare eventuali client** utilizzati per accedere alla gestione dei cloud services;
- **chiedere la collaborazione del provider** (a meno che non sia parte in causa del contenzioso) per acquisire le informazioni che non sono accessibili dall'esterno;
- **documentarsi sulle specifiche dell'ambiente** da analizzare per non trovarsi impreparati nelle fasi successive;
- **acquisire le tipologie di servizi oggetto di indagine e dei servizi di supporto abilitati** (identity and access management, detection and response, network application protection, data protection, compliance and auditing, ecc.);
- **identificare le regioni/zone** che ospitano le virtual machine o le istanze (repliche);
- **leggere il contratto di fornitura** tra utente e provider per comprendere l'oggetto del servizio di cloud, la configurazione del servizio e i service-level agreement.

Collection - Acquisition

Con la voce Collection si intende *"the process of gathering items that contain potential digital evidence"*, ovvero il sequestro di dispositivi che contengono delle potenziali prove digitali; mentre con il termine Acquisition si intende *"the process of creating a copy of data within a defined set*", ovvero la creazione di una copia dei dati che costituiscono delle potenziali prove digitali.

Nel caso specifico, il sequestro è virtuale e potrebbe essere realizzato attraverso la disabilitazione delle utenze admin /user (oppure con il cambio password), l'inibizione dell'accesso agli utenti e il blocco delle VM, delle istanze e dei servizi (a meno che non siano servizi critici), mentre l'acquisizione consente di realizzare una copia delle risorse virtualizzate e dei dati correlati individuati durante la fase di identificazione.

Nei sistemi fisici la copia dei relativi supporti di memoria è realizzata connettendo il dispositivo ad un sistema di acquisizione mediante il quale è creata la copia. Gli ambienti cloud si caratterizzano per l'inaccessibilità fisica delle risorse, la volatilità delle risorse virtualizzate e l'uso di meccanismi di replicazione; pertanto, occorre utilizzare metodologie specifiche.

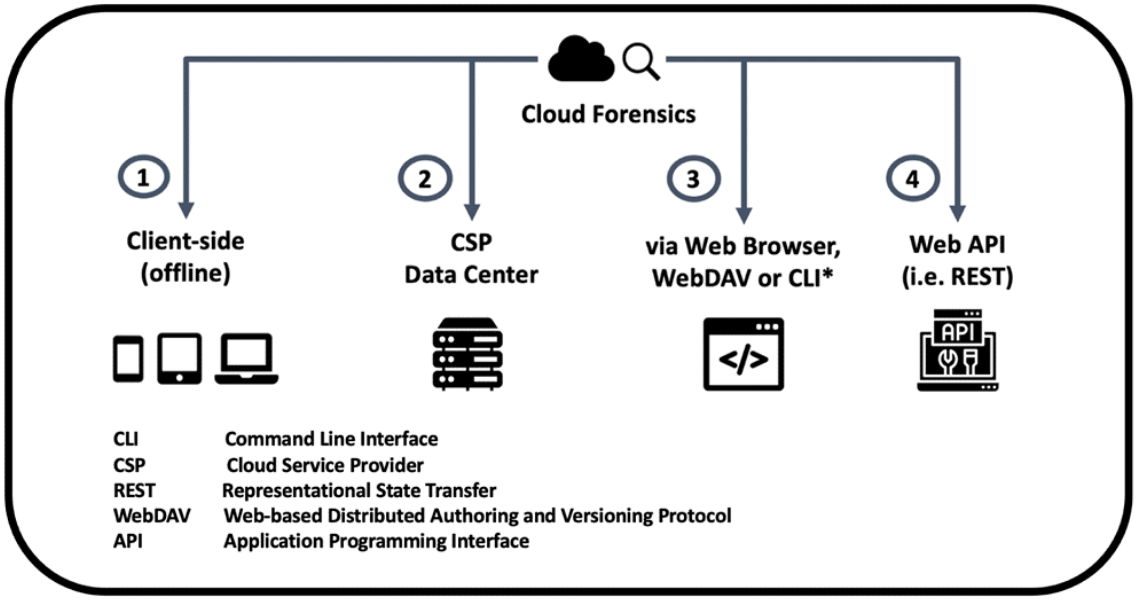
Per risolvere il problema dell'inaccessibilità è necessario acquisire i dati direttamente dall'infrastruttura del provider e, successivamente, essere trasferiti all'esterno del sistema cloud mediante un canale sicuro. Innanzitutto, occorre tenere presente che la realizzazione di questa modalità di acquisizione potrebbero presentarsi problemi di natura legale (transnazionalità), organizzative (interfacciarsi con il provider), tecnica (utilizzo di tecnologie costose e tempistiche ristrette) e forense (violazione di normative).

A riguardo possono essere utilizzate le seguenti tecniche:

- **uso delle interfacce applicative (API)**: i dati vengono acquisiti tramite software che si interfaccia con il sistema cloud attraverso le API (Application Programming Interface) per ottenere una copia delle risorse virtualizzate o dei dati di interesse (per i servizi di tipo SaaS).
- **creazione di una copia della macchina virtuale o del container:** questa operazione può essere realizzata direttamente dal forenser, tramite pannello di gestione, oppure delegata all'amministratore del cloud (per gli altri servizi di tipo IaaS, CaaS, PaaS, FaaS).
- **utilizzo dei tools di controllo**: generalmente i provider offrono strumenti di gestione delle risorse e dei dati accessibili mediante web. Questi tools di controllo consentono di acquisire oltre alla copia della

macchina virtuale o del servizio cloud oggetto di indagine, diversi altri dati utili alla digital forensics, per esempio i file di configurazione delle risorse virtuali, i file di log generati dalla piattaforma, i log relativi agli accessi da parte dell'utente, ecc.

- **uso dei dati per detection & response**: i provider usano tools di monitoring e response per garantire che i loro servizi siano conformi a determinati standard di sicurezza e alle normative vigenti; tali strumenti rappresentano un'ottima fonte di prova e quindi devono essere acquisiti.
- **live forensics**: le piattaforme di virtualizzazione offrono strumenti per l'analisi delle macchine virtuali in esecuzione. Questi strumenti possono essere utilizzati, insieme ai tradizionali strumenti di live forensics, per estrarre varie informazioni direttamente da una macchina virtuale in esecuzione senza perturbarne lo stato.
- **snapshot dello stato**: le macchine virtuali consentono di effettuare lo snapshot, ossia il salvataggio dello stato di una macchina in esecuzione. Questi può contenere diverse informazioni utili quali: i processi in esecuzione, il contenuto della memoria, le sessioni di rete aperte, gli utenti collegati alla macchina virtuale.



Tecniche di acquisizione via API (Fonte: open-research-europe.ec.europa.eu)

Come è noto, i servizi di tipo IaaS e PaaS si basano su risorse virtuali e, per definizione, volatili, pertanto, potrebbero essere facilmente rimosse durante l'acquisizione. Una soluzione a questa criticità è l'utilizzo dello snapshotting già indicato. Ciò presuppone che le risorse di interesse siano individuate in anticipo rispetto alla necessità di acquisizione, prima che vengano rimosse.

Inoltre, occorre tenere conto della duplicazione dei dati. I sistemi cloud sfruttano i meccanismi di replicazione dei dati per offrire adeguati livelli di prestazioni e disponibilità di servizio. La presenza di più repliche dello stesso insieme di dati può causare dei problemi durante l'acquisizione, in quanto i meccanismi di sincronizzazione delle repliche richiedono una congrua quantità di tempo per propagare le modifiche a tutte le altre repliche presenti nel sistema. Pertanto, è necessario che la procedura di acquisizione si interfacci con il gestore delle repliche in modo da ottenere la versione più recente dei dati. Inoltre, è necessario impedire che una qualunque replica venga aggiornata durante l'acquisizione tramite dei meccanismi, se presenti, di lock globali.

Infine, occorre considerare l'aspetto della crittografia. In questi casi dobbiamo prevedere anche l'acquisizione dei client da cui si è avuto accesso al cloud, per acquisire le chiavi di decifratura, ovvero chiedere al cloud provider, nel caso ne fosse provvisto.

Spesso quest'attività è delegata agli specialisti del cloud presso il provider che non hanno quella formazione e sensibilità necessaria per raccogliere e conservare meticolosamente le evidenze in conformità agli standard forensi, preservandone l'integrità e l'autenticità per potenziali procedimenti legali; pertanto, è necessario formarli o affiancarli durante la fase di acquisizione.

Di seguito un elenco, non esaustivo, di tools utilizzabili per l'acquisizione dalle piattaforme cloud: Cado, Google Cloud Forensics Utils, CloudTrail (AWS), Azure Security Center, Azure Activity Log (Azure), Cloud Monitoring (GCP), Magnet AXIOM cloud, Cellebrite UFED cloud analyzer, Mandiant CloudLens, AccessData cloud extractor, Oxygen forensic cloud extractor, ecc.

Preservation

Con la voce Preservation si intende "*the process to maintain and safeguard the integrity and/or original condition of the potential digital evidence*", ovvero la preservazione dell'integrità delle potenziali prove digitali. Dunque, la conservazione di un'acquisizione forense deve garantire l'integrità dei dati, ovvero mantenere le stesse condizioni dell'acquisizione. Lo strumento più utilizzato nella digital forensics a tale scopo è il calcolo dei codici hash crittografici, ma per raggiungere lo stesso obiettivo nel contesto cloud occorre considerare alcune criticità:

- **duplicazione**: la replica dei dati può creare problemi anche in questa fase nel caso in cui non ci siano meccanismi di lock globale, come visto per l'acquisizione.
- **volatilità**: la volatilità crea potenziali criticità in quanto impedisce di preservare lo stato dei dati memorizzati su di esse. L'unica soluzione è creare uno snapshot del sistema.
- **multi-tenancy**: i sistemi cloud si caratterizzano per la condivisione delle risorse tra vari utenti. Questa caratteristica solitamente è compresa nei meccanismi di virtualizzazione, per cui le risorse di ogni utente sono accessibili solo a lui (segregazione), ma non sempre ciò accade, per cui occorre fare attenzione che non vi siano file system o memorie condivise tra più utenti.

Non esiste una soluzione unica a questi problemi, ma è possibile ridurli formando **una dettagliata documentazione delle fasi di acquisizione e conservazione** e, inoltre, utilizzando meccanismi di firma digitale con marca temporale per cristallizzare il momento dell'esecuzione.

Analysis - Presentation

La fase di Analysis consente *"the identification and evaluation of items of evidence from a source of potential digital evidence"*, ovvero l'individuazione e la valutazione di prove digitali, partendo da una sorgente di potenziali prove digitali. Con il termine Presentation si identifica il processo che *"includes describing the actions performed (...) and other aspects of the forensic process"*, ovvero che comprende la descrizione delle azioni effettuate, nonché altri aspetti del procedimento seguito nell'analisi forense. In altri termini, è la presentazione dei risultati.

L'analisi delle evidenze digitali deve essere in grado di individuare e valutare le potenziali prove. Un sistema cloud è caratterizzato dalla presenza di diversi sottosistemi che interagiscono tra loro. Questa integrazione può essere complessa perché le risorse di interesse sono distribuite su diversi dispositivi. Inoltre, un provider può avvalersi di servizi erogati da altri, creando una catena di dipendenze che determina la presenza di possibili potenziali prove su più sistemi cloud.

Risulta determinante effettuare l'integrazione delle diverse fonti di prova per realizzare la ricostruzione completa degli eventi. Alcune soluzioni per effettuare adeguatamente tale integrazione si basano sull'uso di aggregatori dei file di log distinti ed aventi formato eterogeneo.

Spesso è necessario redigere la cosiddetta linea temporale (timeline), ovvero la sequenza degli eventi ordinati cronologicamente in base all'istante della loro occorrenza (timestamp) per ricostruire la successione di eventi verificatisi in un sistema cloud. Poiché gli eventi possono essere generati da dispositivi distinti, è necessario inserire nella stessa linea temporale eventi provenienti da dispositivi diversi. Ciò può essere influito negativamente dalla possibile mancata sincronizzazione degli orologi di sistema oppure dalla difficoltà di associare l'evento a una determinata risorsa. Sarebbe opportuno utilizzare sistemi di logging sicuro.

Inoltre, si può ripresentare il problema della cifratura dei dati. In questa fase le ricadute sono ulteriormente onerose a causa dell'impossibilità di decodificare dati e, quindi, una ricostruzione incompleta degli eventi verificatisi sul sistema.

Conclusioni e prospettive future

L'esposizione delle peculiarità del cloud computing, e delle criticità specifiche di questo ambiente di erogazione dei servizi ICT, ha evidenziato la necessità di scegliere e adottare una metodologia di analisi forense specifica per questi sistemi. Le procedure forensi devono adattarsi ai diversi modelli di erogazione e distribuzione dei servizi, garantendo l'integrità delle evidenze raccolte. La rapida evoluzione degli ambienti cloud richiede un'acquisizione e conservazione tempestiva, per evitare lacune nello svolgimento dell'iter. La solidità della credibilità delle prove si basa sulla loro conservazione sicura.

Dall'analisi emerge chiaramente che vi siano criticità importanti da dover affrontare durante un'indagine digitale. Tra questi, particolare rilievo assumono quelli dovuti alla volatilità delle risorse virtualizzate, quelli determinati dall'inaccessibilità delle risorse fisiche, quelli causati dall'uso di tecniche di cifratura dei dati e, infine, la giurisdizione dei provider. In alcuni casi è fondamentale ottenere il coinvolgimento e il supporto del provider, a meno che non sia una controparte del contenzioso, e sfruttare le tecnologie di detection e response presenti.

Spesso non si distingue l'ambito della Cloud Security da quello della Cloud Forensics. Sono due domini distinti: la cloud security si concentra sulle misure proattive per proteggere i dati e le risorse, tra cui la sicurezza della rete, la crittografia dei dati e il controllo degli accessi, mira a prevenire l'accesso non autorizzato, le violazioni dei dati e le potenziali minacce; la Cloud Forensics, d'altra parte, è un approccio reattivo che indaga e analizza incidenti, violazioni o attività non autorizzate, aiutando le organizzazioni a imparare dalle violazioni e a migliorare il proprio livello di sicurezza. La sicurezza del cloud e la digital forensics condividono alcune tecniche, ma l'analisi forense aderisce rigorosamente alle linee guida legali per l'ammissibilità in tribunale. In una strategia di sicurezza completa è essenziale integrare l'analisi forense per affrontare efficacemente le minacce alla sicurezza come le violazioni dei dati, gli attacchi DDoS e la cattiva condotta degli insider. Pertanto, è indispensabile individuare delle modalità che incentivino i provider all'adozione di procedure che agevolino la produzione e l'acquisizione di evidenze, superando le resistenze che possono frenarne il coinvolgimento e, contemporaneamente, formare i professionisti della sicurezza cloud alla metodologia forense, per evitare che durante un incidente si perdano delle evidenze importanti.

Infine, va ricordato che la cloud forensics presenta problemi di natura giuridica dovuti all'allocazione di risorse virtuali e dati su risorse fisiche ubicate in diversi paesi che devono essere opportunamente approfonditi in altre sedi, al fine di stimolare la ricerca di soluzioni adeguate.

FORUM ICT SECURITY

23-24 OTTOBRE 2024

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
22ª Edizione del Forum ICT Security

ICT Security MAGAZINE

ISCRIVITI ALLA NEWSLETTER

per ricevere aggiornamenti sulle prossime iniziative. Seguici sui canali social: Linkedin, Facebook, Twitter