Conformità al regolamento generale sulla protezione dei dati in AWS

Ottobre 2019

Nota

I clienti sono responsabili della valutazione autonoma delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) mostra le offerte e le pratiche attuali dei prodotti AWS, che potrebbero essere soggette a modifiche senza preavviso e (c) non rappresenta alcun impegno o garanzia da parte di AWS e dai suoi affiliati, fornitori o licenziatari. I prodotti o servizi AWS sono forniti "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia esplicite che implicite. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica di qualsiasi contratto tra AWS e i suoi clienti.

Sommario

Sintesi

Questo documento fornisce informazioni su servizi e risorse che Amazon Web Services (AWS) offre ai suoi clienti, per aiutarli ad allinearsi con i requisiti del Regolamento Generale sulla Protezione Dei dati (GDPR) che potrebbero applicarsi alle loro attività. Questi includono la conformità agli standard di sicurezza IT, l'attestato C5 (Cloud Computing Compliance Controls Catalog) di AWS, il rispetto del Codice di Condotta del Cloud Infrastructure Services Providers in Europe (CISPE), i controlli di accesso ai dati, strumenti di monitoraggio e di logging, la crittografia e la gestione delle chiavi.

Panoramica del Regolamento generale sulla protezione dei dati

Il Regolamento Generale sulla Protezione dei Dati (GDPR) è una legge europea sulla privacy[1] (Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016[2]), entrata in vigore il 25 maggio 2018. Il GDPR sostituisce la Direttiva europea sulla protezione dei dati (Direttiva 95/46/EC) e si prefigge l'obiettivo di armonizzare le leggi relative alla protezione dei dati in tutta l'Unione Europea (UE) con l'adozione di un'unica normativa vincolante in ciascuno Stato membro.

Il GDPR si applica a tutte le attività di elaborazione di dati personali effettuate da organizzazioni con sede legale nell'UE o su dati personali di cittadini residenti nell'UE con lo scopo di offrire beni e servizi a individui nell'UE o monitorare comportamenti di residenti UE nell'UE. Per dati personali si intende qualsiasi informazione relativa a una persona identificata o identificabile.

Cosa cambia per le aziende che operano nell'UE con il *GDPR*

Il GDPR si propone di armonizzare in tutti gli Stati membri le modalità di trattamento, uso e scambio di dati personali in modo sicuro. Le aziende dovranno essere in grado di dimostrare su base continuativa la sicurezza dei dati che trattano e la loro conformità al GDPR, implementando e riesaminando regolarmente le misure tecniche e organizzative, oltre a opportune policy di conformità applicabili al trattamento dei dati personali. In caso di violazione del GDPR, le autorità europee di controllo potranno emettere ammende fino a 20 milioni di euro o pari al 4% del fatturato annuo in tutto il mondo, se maggiore.

Preparazione di AWS per il GDPR

Gli esperti AWS su conformità e sicurezza lavorano con clienti di tutto il mondo, rispondendo alle loro domande e aiutandoli a gestire i loro carichi di lavoro sul cloud nel rispetto del GDPR. Questi team si occupano anche di esaminare le responsabilità di AWS alla luce dei requisiti del GDPR.

> Siamo in grado di confermare che tutti i servizi AWS possono essere utilizzati in conformità con il GDPR.

Addendum sul trattamento dei dati (DPA) di AWS

AWS offre un Addendum sul trattamento dei dati conforme al GDPR (GDPR DPA), che consente di soddisfare gli obblighi contrattuali stabiliti dal GDPR. L'Addendum di AWS al GDPR è integrato nei Termini del servizio AWS e viene applicato automaticamente a tutti i clienti che, in tutto il mondo, ne hanno bisogno per essere conformi al GDPR.

Il ruolo di AWS nell'ambito del GDPR

AWS agisce come titolare e come responsabile del trattamento di dati nell'ambito del GDPR.

AWS come responsabile del trattamento di dati

Quando clienti e Solution Provider AWS utilizzano i servizi AWS per elaborare dati personali nei loro contenuti, AWS funge da responsabile del trattamento dei dati. I clienti e i Solution Provider AWS possono utilizzare i controlli disponibili nei servizi AWS, inclusi i controlli di configurazione della sicurezza, per la gestione delle informazioni personali. In questi casi, il cliente o Solution Provider AWS può agire come titolare o responsabile del trattamento dei dati e AWS agisce come responsabile principale o secondario del trattamento dei dati. L'Addendum di AWS sul trattamento dei dati conforme al GDPR (DPA) include gli impegni di AWS come responsabile del trattamento dei dati.

AWS come titolare del trattamento dei dati

AWS funge da titolare del trattamento dei dati quando raccoglie dati personali e ne determina gli obiettivi e la modalità di trattamento. Ad esempio, AWS agisce da titolare del trattamento dei dati quando raccoglie informazioni sugli account per la registrazione, la gestione, l'accesso ai servizi, il contatto e il supporto dei clienti.

Ai sensi dell'articolo 32, i titolari e i responsabili del trattamento sono tenuti a "[mettere] in atto misure tecniche e organizzative adeguate [...] tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche". Il GDPR include suggerimenti specifici sui tipi di azioni di sicurezza che possono essere richiesti, ad esempio:

- La pseudonimizzazione e la crittografia dei dati personali.
- La capacità di garantire riservatezza, integrità, disponibilità e resilienza di sistemi e servizi di elaborazione in modo continuo.

- La possibilità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di problema tecnico o fisico.
- Una procedura per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Modello di responsabilità condivisa della sicurezza

La responsabilità in materia di sicurezza e conformità è condivisa tra AWS e il cliente. Quando un cliente trasferisce sistemi informatici e dati nel cloud, le responsabilità di sicurezza vengono condivise tra il cliente e il fornitore di servizi cloud. Quando il cliente migra al cloud AWS, AWS è responsabile della sicurezza dell'infrastruttura che supporta il cloud, mentre il cliente è responsabile per qualsiasi cosa venga caricata sul cloud o collegata a esso. La suddivisione delle responsabilità è generalmente indicata come sicurezza del cloud versus sicurezza nel cloud.

Il modello condiviso può aiutare a ridurre l’onere operativo a carico del cliente, fornendogli la flessibilità e il controllo necessari allo sviluppo delle infrastrutture nel cloud AWS. AWS opera, gestisce e controlla i componenti dell'infrastruttura, dal sistema operativo host e il livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui operano i servizi. Al cliente spetta la responsabilità e la gestione del sistema operativo guest (con relativi aggiornamenti e patch di sicurezza), di altri software applicativi associati e della configurazione del firewall del gruppo di sicurezza fornito da AWS. Per ulteriori informazioni, visita la pagina del Modello di responsabilità condivisa AWS.

Framework rigorosi di conformità e standard di sicurezza

Ai sensi del GDPR, può essere necessario includere nelle misure tecniche e organizzative appropriate "la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione su base continuativa", nonché l'affidabilità dei processi di ripristino, test e di gestione generale del rischio.

Programma AWS Compliance

La conformità AWS aiuta i clienti a capire i solidi sistemi di controllo messi in atto da AWS per mantenere sicurezza e protezione dei dati nel cloud AWS. Quando viene costruito un sistema nel cloud AWS, le responsabilità in merito alla conformità sono condivise. Mettendo insieme funzionalità di servizi basate su governance e che facilitano processi di audit, con gli strumenti per la conformità di AWS (come AWS Config, AWS CloudTrail, AWS Identity and Access Management, Amazon GuardDuty e AWS Security Hub) standard di audit; basandosi su programmi tradizionali i clienti, hanno la possibilità di lavorare nell'ambiente protetto di AWS. L'infrastruttura IT che AWS fornisce ai suoi clienti è progettata e gestita secondo le migliori pratiche di sicurezza e nel rispetto di una serie di standard di sicurezza IT, tra cui:

- SOC 1/SSAE 16/ISAE 3402 (precedentemente SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP e FedRAMP
- DoD SRG
- PCI DSS livello 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Tier 3

Le caratteristiche di flessibilità e controllo offerte dalla piattaforma AWS consentono ai clienti di distribuire soluzioni in grado di rispondere a molti standard specifici per diversi settori[3].

AWS fornisce ai clienti una vasta gamma di informazioni sul proprio ambiente di controllo IT, tramite whitepapers, reports, certificazioni, accreditamenti e altre attestazioni di terze parti. Per ulteriori informazioni, consulta il whitepaper Amazon Web Services: rischio e conformità.

Cloud Computing Compliance Controls Catalog

Il Cloud Computing Compliance Controls Catalog (C5) è uno schema tedesco di attestazione riconosciuto dal governo introdotto in Germania dal Federal Office for Information Security (BSI). È stato creato per aiutare le organizzazioni a dimostrare la sicurezza a livello operativo rispetto agli attacchi informatici comuni nell'ambito delle Security Recommendations for Cloud Providers del governo tedesco.

Le misure tecniche e organizzative della protezione dei dati e le misure per la sicurezza delle informazioni si concentrano sulla sicurezza dei dati per garantire riservatezza, confidenzialità, integrità e disponibilità. C5 definisce i requisiti di sicurezza importanti anche per la protezione dei dati. L'attestazione può essere utilizzata dai clienti AWS e dai rispettivi consulenti sulla conformità per comprendere la gamma di servizi di assicurazione per la sicurezza IT offerti da AWS durante il trasferimento dei carichi di lavoro nel cloud. C5 aggiunge il livello di sicurezza IT definito a livello normativo equivalente allo standard IT-Grundschutz, con l'aggiunta di controlli specifici per il cloud.

C5 prevede controlli aggiuntivi che forniscono informazioni riguardo a dove risiedono i dati, al provisioning dei servizi, alla giurisdizione di riferimento, ad eventuali certificazioni esistenti, agli obblighi di non divulgazione delle informazioni e una descrizione completa del servizio. Utilizzando queste informazioni, i clienti possono valutare in che modo le normative legali (ad esempio quelle riguardanti la privacy dei dati), le proprie politiche o l'ambito delle minacce sono connessi all'utilizzo dei servizi di cloud computing.

Codice di condotta CISPE

Il GDPR permette di effettuare l'approvazione di alcuni codici di condotta per aiutare i titolari e i responsabili del trattamento dati a dimostrare la conformità alle norme vigenti. Uno di questi codici, in attesa di approvazione ufficiale dalle autorità europee per la protezione dei dati, è il Codice di condotta CISPE per i fornitori di servizi di infrastruttura cloud (il Codice)[4]. Il Codice rassicura i clienti perché dimostra che il loro fornitore di servizi cloud adotta standard di protezione dati idonei e conformi al GDPR.

Alcuni dei vantaggi del Codice:

- ***Chiarisce chi è responsabile per ciascun aspetto della protezione dei dati*** - Il Codice spiega il ruolo del fornitore e del cliente nell'ambito del GDPR, in particolare per quanto riguarda i servizi infrastrutturali cloud.
- ***Definisce i principi a cui i fornitori si devono attenere*** - Il Codice sviluppa i principi fondamentali del GDPR individuando le attività che i fornitori devono svolgere e gli impegni che si devono assumere per dimostrare la propria conformità al GDPR e aiutare i clienti a garantirla a loro volta. I clienti possono sfruttare questi vantaggi concreti nelle loro strategie di conformità e protezione dei dati.
- ***Fornisce ai clienti informazioni relative alla sicurezza, necessarie ad aiutarli a raggiungere i loro obiettivi di conformità*** - Il Codice richiede che i fornitori siano trasparenti in merito alle fasi intraprese per rispettare i loro impegni nell'ambito della sicurezza e della privacy. Alcune di tali fasi includono l'implementazione di strumenti per la protezione della privacy e della sicurezza, per la notifica in caso di violazione di dati, eliminazione di dati e per la trasparenza in caso di trattamento dei dati a un livello inferiore da parte di terze parti. Tutti questi impegni sono soggetti a verifica da parte di entità di controllo esterne e indipendenti. I clienti possono utilizzare queste informazioni per acquisire una conoscenza approfondita degli elevati livelli di sicurezza forniti.

Al momento della pubblicazione di questo documento, AWS ha registrato Amazon EC2, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), AWS CloudTrail e Amazon Elastic Block Store (Amazon EBS) come pienamente conformi al Codice. Per ulteriori informazioni, consultare il Registro pubblico CISPE. Questo rassicura ulteriormente i clienti riguardo la loro capacità di controllare i loro dati in un ambiente protetto, sicuro e conforme quando usano AWS. La conformità di AWS al Codice si aggiunge alla lista di certificazioni e accreditamenti riconosciuti a livello internazionale che AWS ha ottenuto. Tra questi figurano: ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3, PCI DSS Livello 1, ecc.

Controllo dell'accesso ai dati

L'articolo 25 del GDPR stabilisce che il titolare del trattamento " mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.” I seguenti meccanismi AWS per il controllo dell’accesso possono aiutare i clienti a soddisfare questo requisito, concedendo l’accesso alle risorse AWS e ai dati dei clienti esclusivamente alle applicazioni, agli amministratori e agli utenti autorizzati.

AWS Identity and Access Management

Al momento della creazione di un account AWS, a questo viene automaticamente associato un utente root. Tale account gode di accesso completo a tutti i servizi e risorse AWS disponibili per quell’account AWS. Invece di usare questo account per tutte le attività, è consigliabile utilizzarlo in una prima fase per creare ruoli e utenti aggiuntivi e per compiere attività amministrative per le quali sono necessari privilegi di root. AWS consiglia di applicare fin da subito il principio del privilegio minimo. Tale principio consiste diversi utenti e ruoli per diverse attività e specificare l’insieme minimo di permessi necessari per completare ciascuna attività. Tale approccio è un meccanismo che consente di introdurre un concetto cardine del GDPR: introdurre processi per la protezione dei dati fin dalla progettazione (data protection by design). AWS Identity and Access Management (IAM) è un servizio web che puoi usare per controllare in modo sicuro l'accesso alle tue risorse AWS.

Utenti e ruoli definiscono identità IAM con permessi specifici. Con i ruoli IAM è possibile permettere a qualsiasi utente di compiere attività specifiche, sfruttando credenziali temporanee per la sessione del ruolo. I ruoli IAM possono essere utilizzati per fornire ad applicazioni che sfruttano Amazon EC2 le credenziali necessarie per ottenere l’accesso ad altre risorse AWS, come bucket Amazon S3 o i database Amazon RDS o DynamoDB.

Token di accesso temporaneo attraverso AWS STS

AWS Security Token Service (AWS STS) consente di creare credenziali di sicurezza provvisorie e assegnarle a utenti fidati per permettere loro di accedere alle risorse AWS. Le credenziali di sicurezza provvisorie funzionano in modo quasi identico alle credenziali delle chiavi di accesso a lungo termine che si forniscono agli utenti IAM, tranne per le seguenti differenze:

- Le credenziali di sicurezza provvisorie sono a breve termine. È possibile personalizzare la durata della validità di queste credenziali: da pochi minuti a diverse ore. Dopo la scadenza delle credenziali provvisorie, AWS non le riconosce più né consente alcun tipo di accesso dalle richieste API che le utilizzano.
- Le credenziali di sicurezza temporanee non vengono salvate insieme all'account dell'utente. Sono, invece, generate in maniera dinamica e fornite all'utente su richiesta. Una volta scadute le credenziali di sicurezza provvisorie, o prima che ciò avvenga, l'utente può richiederne di nuove, se tale utente ha i permessi per farlo.

Queste differenze fanno sì che le credenziali provvisorie presentino i seguenti vantaggi:

- Non occorre distribuire o allegare credenziali di sicurezza AWS a lungo termine con un'applicazione.
- Le credenziali provvisorie sono la base dei ruoli e della federazione delle identità. È possibile concedere agli utenti l'accesso alle tue risorse AWS definendo per loro un'identità AWS provvisoria.
- Le credenziali di sicurezza provvisorie hanno una validità limitata e personalizzabile. Pertanto, non è necessario ruotarle o revocarle in modo esplicito quando non sono più necessarie. Quando le credenziali di sicurezza provvisorie scadono, non possono essere riutilizzate. Il tempo massimo di validità per le credenziali è personalizzabile.

Multi-Factor Authentication

Per ulteriore sicurezza, è disponibile un'autenticazione a due fattori da aggiungere all'account root e ai singoli utenti. Una volta attivata la Multi-Factor Authentication (MFA), l'accesso al sito AWS avviene dopo l'inserimento di user name e password (primo fattore), insieme a un input per l'autenticazione da parte del tuo dispositivo MFA AWS (secondo fattore). La MFA può essere impostata per l'account AWS e per i singoli utenti IAM creati nell'account. La MFA consente anche di controllare gli accessi ai servizi API di AWS.

Ad esempio, è possibile definire una policy che consente un accesso totale a tutte le operazioni che avvengono tramite API AWS in Amazon EC2, negando esplicitamente l'accesso per specifiche operazioni API (ad esempio StopInstances e TerminateInstances) se l'utente non ha eseguito l'accesso con l'MFA.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllActionsForEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

Figura 1 – Richiesta di MFA per specifiche operazioni API su Amazon EC2

Accesso alle risorse per gli oggetti AWS

Per implementare un accesso granulare a oggetti AWS, si possono assegnare autorizzazioni diverse a persone diverse per risorse diverse. Ad esempio, concedendo solo ad alcuni utenti l'accesso completo ad Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift e altri servizi AWS.

Altri utenti, invece, possono essere autorizzati ad accedere in modalità di sola lettura solo ad alcuni bucket Amazon S3, a gestire solo alcune istanze EC2 o ad accedere limitatamente e solo alle informazioni di fatturazione.

La seguente policy rappresenta un esempio di un metodo utilizzabile per permettere tutte le azioni a un bucket specifico di Amazon S3 e negare esplicitamente l'accesso a ogni servizio AWS che non sia Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        },
        {
            "Effect": "Deny",
            "NotAction": "s3:*",
            "NotResource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Figura 2 – *Limitare l'accesso* un bucket specifico Amazon S3

Le policy possono essere associate a un account utente o a un ruolo. Per altri esempi di policy IAM, consultare Esempi di policy basate su identità IAM.

Accesso a dati operativi e di configurazione

AWS System Manager può essere usato per visualizzare e gestire le operazioni su infrastruttura AWS. Consente di testare e mettere in atto la conformità rispetto a stati definiti. AWS Systems Manager Parameter Store permette di gestire a livello centrale i dati attraverso la definizione di parametri. Ciò permette di implementare un accesso granulare ai parametri, siano essi dati sotto forma di testo semplice (come stringhe di database) o credenziali di accesso (come ad esempio le password). E' possibile realizzare permessi personalizzati per utenti e risorse (come le istanze) per consentire a questi di accedere ai parametri definiti sfruttando l'integrazione con IAM. Ad esempio, in un ambiente di sviluppo, le credenziali sono spesso disseminate all'interno del codice; Parameter Store consente di salvare le password in un unico punto e permette agli sviluppatori di avere accesso alle credenziali con AWS API get-parameter.

Di seguito si riporta un esempio di utilizzo del comando get-parameter per il recupero della password:

```
password=$(aws ssm get-parameters --region us-east-1 --names MySecureSQLPassword
```

Un'altra opzione disponibile per proteggere i credenziali necessarie per accedere ad applicazioni, servizi e risorse IT è AWS Secrets Manager. Questo servizio permette di ruotare, gestire e recuperare facilmente le credenziali di un database, le chiavi API e altre tipologie di credenziali di accesso nel corso del loro ciclo di vita. Utenti e applicazioni recuperano le credenziali chiamando le API di Secrets Manager, il che elimina la necessità di includere informazioni confidenziali in formato testo. Secrets Manager supporta la rotazione delle credenziali ed è integrato con Amazon RDS, Amazon Redshift e Amazon DocumentDB.

Restrizioni geografiche

Puoi utilizzare restrizioni geografiche - note anche come geoblocking - per impedire a utenti in specifiche aree geografiche di accedere a contenuti che stai distribuendo tramite una distribuzione web Amazon CloudFront.

Ci sono due opzioni per utilizzare le restrizioni geografiche:

- ***Modalità di restrizione geografica su CloudFront*** - Questa opzione limita l'accesso a tutti i file associati a una distribuzione CloudFront e limita l'accesso a livello di paese.
- ***Servizi di geolocalizzazione di terze parti*** - Questa opzione limita l'accesso a un sottoinsieme di file associati a una distribuzione o a un livello di granularità più fine rispetto a quello di paese.

Oltre queste due opzioni, esistono funzionalità di geo-limitazione per regioni appena lanciate. Le regioni AWS introdotte prima del 20 marzo 2019 sono abilitate per impostazione predefinita. Le regioni introdotte dopo il 20 marzo 2019, come Asia Pacifico (Hong Kong) e Medio Oriente (Bahrain) sono disabilitate per impostazione predefinita. Queste regioni devono essere abilitate per poter essere utilizzate. Se una regione AWS è disabilitata per impostazione predefinita, è possibile utilizzare la Console di gestione AWS per abilitarla e disabilitarla. Abilitare e disabilitare una regione AWS permette di verificare che gli utenti dell'account AWS possano accedere alle risorse di quella regione.[5]

Controllo accessi ad applicazioni web e applicazioni mobile

AWS offre un servizio per gestire l'accesso ai dati all'interno delle applicazioni. Per aggiungere una funzione di login per un utente e controllo accesso a una applicazione web e app mobile, è possibile usare Amazon Cognito. I pool di utenti di Amazon Cognito forniscono una directory utente sicura e in grado di ricalibrare le risorse per centinaia di milioni di utenti. Per proteggere l'identità degli utenti, la Multi-Factor Authentication (MFA) può essere applicata al pool di utenti. L'autenticazione adattiva sfrutta un modello basato sul rischio per prevedere quando potrebbe essere necessario inserire la seconda fase di autenticazione.

Amazon Cognito dà la possibilità di verificare chi ha effettuato l'accesso alle risorse e dove è avvenuto tale accesso (applicazioni mobile o applicazioni web). Queste informazioni possono essere utili per creare policy di sicurezza che accordano e vietano l'accesso alle risorse a seconda del tipo di origine dell'accesso (da applicazione mobile o web).

Monitoraggio e logging

L’articolo 30 del GDPR afferma che "ogni titolare del trattamento e, ove applicabile, il suo rappresentante devono tenere un registro delle attività di trattamento di cui sono responsabili”. Questo articolo include anche dettagli su quali informazioni debbano essere registrate durante il controllo del trattamento dei dati personali, come richiesto dal GDPR. Il titolare e il rappresentante del trattamento devono anche inviare tempestivamente notifiche in caso di incidenti di sicurezza, quindi è fondamentale che questi siano tempestivamente rilevati. Per aiutare i clienti a garantire la conformità a tali obblighi, AWS offre i seguenti servizi relativi a monitoraggio e logging.

Gestione e configurazione di risorse con AWS Config

AWS Config fornisce una visualizzazione dettagliata della configurazione delle risorse AWS di un account AWS. Ciò include il modo in cui le risorse sono correlate tra loro e in cui sono state configurate in passato, al fine di permettere di evidenziare come questi due elementi cambiano nel tempo ed accorgersi di eventuali modifiche alla configurazione.

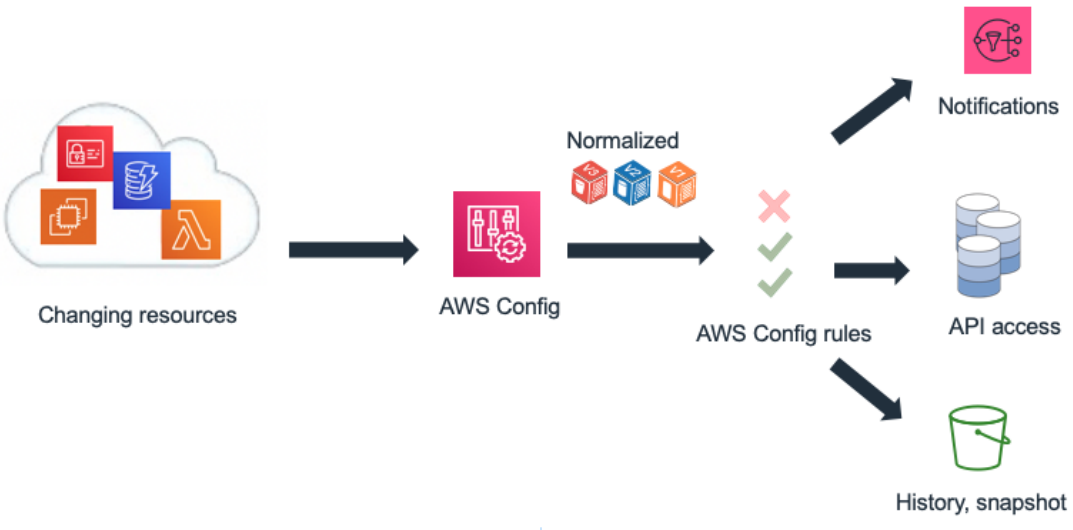

Figura3 - I cambiamenti nel tempo della configurazione con AWS Config

Per risorsa AWS si intende un'entità con la quale si può lavorare in AWS, ad esempio un'istanza Amazon Elastic Compute Cloud (EC2), un volume Amazon Elastic Block Store (EBS), un security group o un Amazon Virtual Private Cloud (VPC). Per un elenco completo delle risorse AWS supportate da AWS Config, consulta la pagina sulle Tipologie di risorse AWS supportate.

AWS Config consente di effettuare le seguenti operazioni:

- Valutare le configurazioni delle tue risorse AWS rispetto alle impostazioni desiderate.
- Ottenere un' istantanea delle configurazioni attuali delle risorse supportate associate al tuo account AWS.
- Ripristinare configurazioni di una o più risorse esistenti per il tuo account.
- Ripristinare le configurazioni preesistenti di una o più risorse.
- Ricevere una notifica ogni volta che una risorsa viene creata, modificata o eliminata.
- Visualizzare le relazioni fra le risorse. Ad esempio, è possibile trovare tutte le risorse che usano un security group specifico.

Audit sulla conformità e analisi della sicurezza con AWS CloudTrail

Con AWS CloudTrail è possibile monitorare in maniera continuativa l'attività di un account AWS. CloudTrail fornisce lo storico delle chiamate API AWS di un account, comprese quelle effettuate tramite la Console di gestione di AWS, l' SDK di AWS, gli strumenti a riga di comando e altri servizi AWS di livello superiore. È possibile identificare quali utenti e account hanno richiamato le API per i servizi che supportano AWS CloudTrail, l'indirizzo IP sorgente da cui sono state effettuate le chiamate e quando sono avvenute. È possibile integrare CloudTrail nelle applicazioni usando le API, automatizzare la creazione di tracce di log per la propria organizzazione, verificarne lo stato e controllare come gli amministratori attivano o disattivano la generazione di log con CloudTrail. I log CloudTrail possono essere organizzati e salvati in bucket Amazon S3 per scopi di auditing o per attività di risoluzione dei problemi.

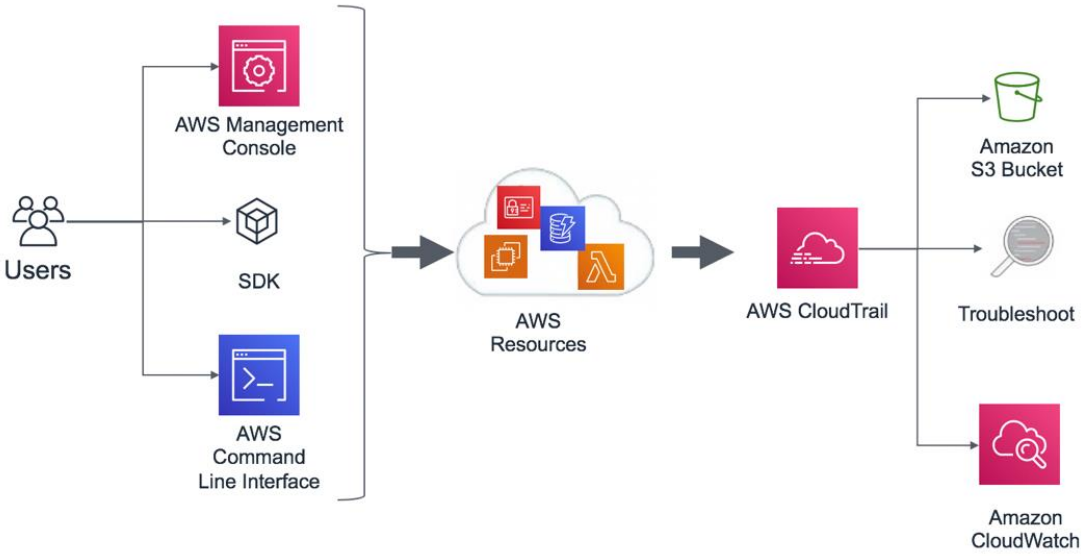

Figura 4 – *Esempio di un'architettura per audit sulla conformità e analisi sulla sicurezza con* AWS CloudTrail

I log AWS CloudTrail possono anche generare eventi Amazon CloudWatch preconfigurati. Questi eventi possono essere utilizzati per inviare notifiche a utenti o sistemi nel caso in cui si verifichi un evento o per richiedere azioni correttive. Ad esempio, per monitorare le attività sulle istanze Amazon EC2, è possibile creare una Event Rule su CloudWatch. Quando si effettua un'attività specifica sull'istanza Amazon EC2 e l'evento viene registrato nei log, la regola avvia una funzione AWS Lambda, che invia un messaggio di notifica contenente informazioni sull'evento (quando si è verificato, quale utente ha compiuto l'azione, dettagli sull'istanza Amazon EC2, ecc.) all'amministratore. Il diagramma in basso mostra l'architettura della notifica sull'evento.

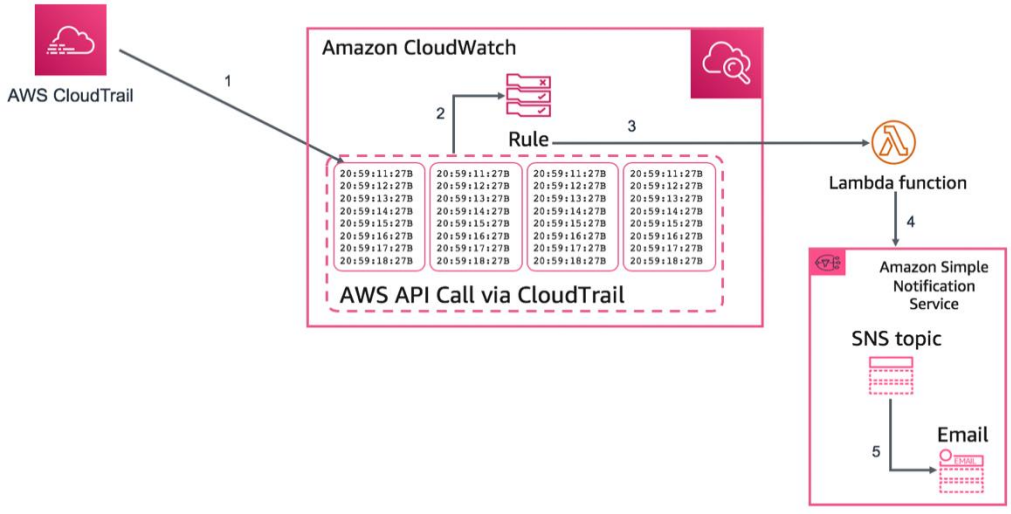

Figura5 - Esempio di notifica su un evento AWS CloudTrail

Formati dei Log

Attivare il logging consente di ottenere log di accesso dettagliati per le richieste effettuate da un bucket Amazon S3. Uno storico dei log di accesso contiene i dettagli della richiesta, come il tipo di richiesta, le risorse specificate nella richiesta, ora e data in cui la richiesta è stata elaborata. Per ulteriori informazioni sui contenuti di un messaggio sui log, consultare la sezione Formato dei log di accesso al server Amazon S3 nella guida per sviluppatori di Amazon Simple Storage Service.

I log di accesso al server sono utili per molte applicazioni, perché offrono ai proprietari del bucket informazioni sulla natura delle richieste fatte dai clienti che non sono sotto il loro controllo. Per impostazione predefinita, Amazon S3 non raccoglie i log di accesso al servizio, ma quando si abilita la registrazione di log, Amazon S3 distribuisce i log di accesso al bucket con frequenza oraria.

Queste informazioni includono:

- Registrazione granulare di log per gli accessi a oggetti Amazon S3
- Informazioni dettagliate sui flussi nella rete tramite i log di flusso di VPC.
- Controlli e azioni delle configurazioni basati su regole con AWS Config Rules.
- Filtro e monitoraggio degli accessi HTTP alle applicazioni con funzioni WAF in CloudFront

I log sono anche un'utile fonte di informazioni per il rilevamento delle minacce. Amazon GuardDuty analizza i log provenienti da AWS CloudTrail, VPC Flow Logs e AWS DNS, permettendo di monitorare costantemente gli account AWS e il carico di lavoro. Questo servizio sfrutta meccanismi di machine learning, di rilevamento intelligente di minacce ed anomalie per fornire avvisi dettagliati e risolvibili tramite azioni ogni volta che viene rilevata un'attività maligna o un comportamento non autorizzato.

Gestione centralizzata della sicurezza

Molte organizzazioni si ritrovano ad affrontare sfide legate alla visibilità e alla gestione centralizzata del loro ambiente. L'aumentare delle dimensioni dell'organizzazione può comportare un peggioramento di questa sfida, a meno che non si progetti attentamente un approccio alla sicurezza. La mancanza di conoscenza, unita a una gestione decentralizzata e disomogenea dei processi di governance e sicurezza, può rendere un ambiente vulnerabile.

AWS offre strumenti per aiutare i clienti a soddisfare alcuni dei requisiti più complessi nella gestione e nella governance IT, oltre a strumenti per supportare un approccio alla protezione dei dati "by design", che considera la sicurezza già dalla fase di progettazione.

AWS Control Tower offre un metodo semplice per creare e gestire un ambiente AWS nuovo, sicuro e con account multipli. Automatizza la creazione di una landing zone[6], che rappresenta un ambiente con account multipli che supporta la governance attraverso l'utilizzo di "guardrails" selezionabili da una lista prefedinita. Le "guardrails" implementano regole di governance per sicurezza, conformità e processi operativi create secondo best-practices. AWS Control Tower permette una gestione delle identità tramite la directory predefinita di AWS Single Sign-On (SSO) e consente l'audit tra più account con AWS SSO e AWS IAM. Centralizza, inoltre, i log provenienti da Amazon Cloudtrail e AWS Config, che sono salvati in Amazon S3.

AWS Security Hub è un altro servizio che supporta la centralizzazione e può migliorare la visibilità su un'organizzazione. Security Hub centralizza e ordina in base alle priorità i risultati sulla sicurezza e la conformità provenienti dai vari account e servizi AWS. Inoltre, può essere integrato con software per la sicurezza di partner terzi per consentire l'analisi delle minacce e l'identificazione dei problemi prioritari relativi alla sicurezza.

Amazon CloudWatch Events consente di impostare su un account AWS l'invio di eventi ad altri account AWS o diventare un destinatario di eventi inviati da altri account o organizzazioni. Questo meccanismo può essere molto utile per implementare scenari trasversali di risposta agli incidenti, in quanto permette di intraprendere rapidamente azioni correttive (ad esempio, chiamando una funzione Lambda o eseguendo un comando su un'istanza EC2) a seconda delle necessità, ogni volta che si verifica un incidente alla sicurezza.

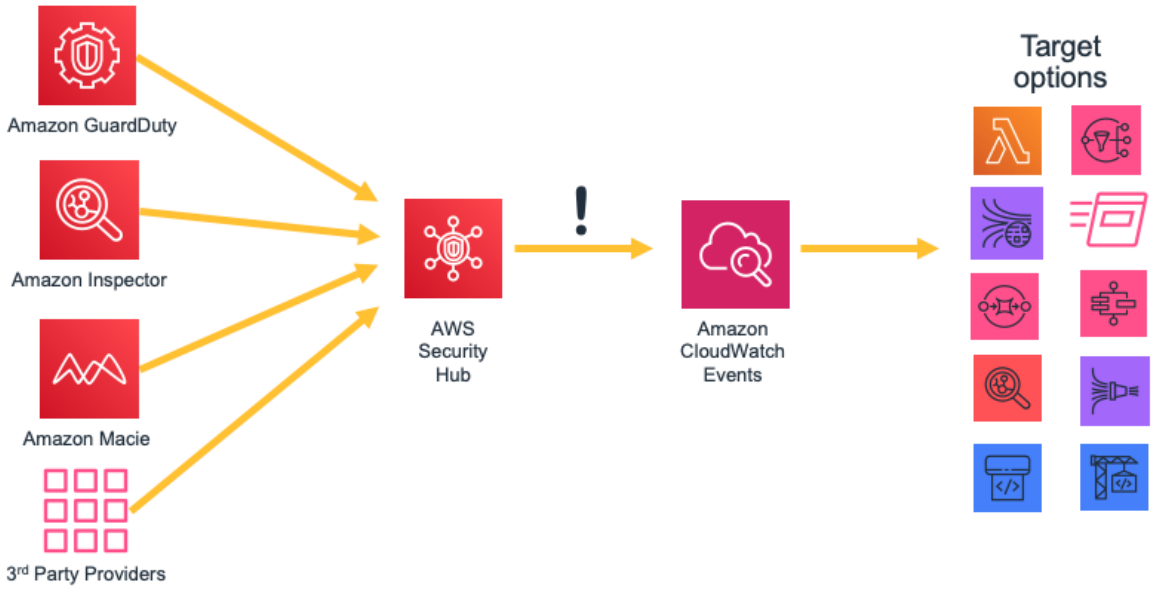

Figura 6 – Intraprendere azioni con AWS Security Hub e Amazon CloudWatch Events

AWS Organizations aiuta a gestire e governare ambienti molto complessi in maniera centralizzata. Permette di controllare accessi, conformità e sicurezza in un ambiente con account multipli. AWS Organizations supporta le Policy di controllo dei servizi (SCP), che definiscono le azioni che è possibile intraprendere sui servizi AWS utilizzando i diversi account appartenenti a un'organizzazione.

Protezione dei dati in AWS

L’articolo 32 del GDPR prevede che le organizzazioni debbano "[mettere] in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono [...] la pseudonimizzazione e la cifratura dei dati personali” Inoltre, le organizzazioni sono tenute a tutelarsi contro la divulgazione o l'accesso non autorizzati ai dati personali.

La cifratura riduce i rischi associati alla conservazione dei dati personali, perché rende i dati illeggibili, salvo possesso della chiave corretta. Una strategia di cifratura a 360° può aiutare a ridurre l’impatto degli incidenti di sicurezza, inclusi alcune security breaches.

Cifratura di dati a riposo

La cifratura di dati a riposo è un processo vitale per la conformità normativa e la protezione dei dati. Aiuta a far sì che i dati sensibili salvati su dischi non siano accessibili a utenti o applicazioni non in possesso di un chiave valida. AWS offre varie opzioni per la cifratura dei dati a riposo e la gestione delle chiavi di cifratura. Ad esempio, è possibile utilizzare AWS Encryption SDK con una chiave master del cliente (CMK), creata e gestita all’interno di AWS Key Management Service (AWS KMS), per codificare dati arbitrari.

I dati codificati possono essere conservati a riposo in modo sicuro e la loro decodifica può avvenire solo da parte di un soggetto con accesso autorizzato alla CMK. Il risultato è la codifica dei dati confidenziali, un meccanismo di policy per l’autorizzazione e la cifratura autenticata oltre che un logging di audit tramite AWS Cloudtrail. Alcuni servizi base di AWS integrano le funzioni di cifratura di dati a riposo, fornendo l’opzione di codificare i dati prima di scriverli in archivi non volatili. Ad esempio, si possono crittografare volumi Amazon Elastic Block Store (Amazon EBS) e configurare bucket Amazon Simple Storage Service (Amazon S3) per la crittografia lato server (SSE) usando la crittografia AES-256. Anche Amazon Relational Database Service (Amazon RDS) supporta la Transparent Data Encryption (TDE).

Un altro metodo per cifrare i dati su instance store Linux EC2 è l'utilizzo di librerie Linux integrate. Questo metodo consente di crittografare i file in modo trasparente, proteggendo i dati riservati. Di conseguenza, le applicazioni che trattano i dati ignorano la cifratura esistente a livello del disco.

È possibile usare due metodi per criptare file in instance store. Il primo metodo consiste nella cifratura del disco, che si effettua sull’intero disco o su un blocco al suo interno usando almeno una chiave crittografica. La cifratura del disco opera al di sotto del livello

file system, non si basa su un sistema operativo specifico e nasconde informazioni su directory e file, come nome e dimensione. Encrypting File System, ad esempio, è un'estensione Microsoft del New Technology File System (NTFS) del sistema operativo Windows NT che fornisce crittografia del disco.

Il secondo metodo consiste nella crittografia a livello di file system. Questo metodo realizza una crittografia dei file e delle cartelle ma non di tutto il disco o di tutta la partizione. La crittografia a livello di file system opera sul file system ed è trasferibile da un sistema operativo all'altro.

Per volumi di instance store SSD di tipo Non-Volatile Memory Express (NVMe), la codifica è un'opzione predefinita. I dati sull'instance storage NVMe sono crittografati utilizzando un codice di blocco XTS-AES-256 implementato su un modulo hardware sull'istanza. Le chiavi di crittografia vengono generate utilizzando il modulo hardware e sono univoche per ogni dispositivo dell'instance storage NVMe. Tutte le chiavi di crittografia vengono distrutte quando l'istanza viene arrestata o terminata e non possono essere recuperate. Non è possibile usare chiavi di crittografia personali.

Crittografia di dati in transito

AWS consiglia caldamente di codificare i dati in transito da un sistema all'altro, includendo risorse all'interno e all'esterno di AWS.

Quando viene creato un account AWS, a esso viene riservata una sezione logicamente isolata del cloud AWS, chiamata Amazon Virtual Private Cloud (Amazon VPC). In quest'area è possibile lanciare risorse AWS in una rete virtuale definita dal cliente. Questi ha il controllo completo sull'ambiente virtuale di rete. Ciò permette di selezionare l'intervallo di indirizzi IP, creare subnet e configurare tabelle di routing e gateway di rete. Inoltre, è possibile creare una connessione VPN hardware tra il data center aziendale e la VPC Amazon per utilizzare il cloud AWS come estensione del data center aziendale.

Per proteggere la comunicazione tra la VPC Amazon e il data center aziendale, è possibile scegliere tra diverse opzioni di connettività VPN quella che meglio soddisfa le proprie necessità. AWS VPN Client consente un accesso sicuro alle risorse AWS attraverso servizi VPN con base client. È possibile anche usare un dispositivo software VPN di terze parti da installare su un'istanza Amazon EC2 sulla VPC Amazon. In alternativa, è possibile creare una connessione VPN IPsec tra il cloud VPC e la rete remota. AWS Direct Connect consente di creare una connessione privata dedicata da una rete remota e la VPC Amazon. Questa connessione può essere abbinata a una connessione VPN site-to-site per creare una connessione crittografata IPsec.

AWS fornisce degli endpoint HTTPS tramite il protocollo TLS (Transport Layer Security) per le comunicazioni, il che offre una codifica in transito quando si usano le API AWS. Il servizio AWS Certificate Manager (ACM) consente di generare, gestire e distribuire certificati privati e pubblici da utilizzare per stabilire un trasferimento cifrato tra i sistemi tra cui si muove un carico di lavoro. Amazon Elastic Load Balancing, integrato in ACM, può essere utilizzato come supporto per i protocolli HTTPS. Se un contenuto viene distribuito tramite Amazon CloudFront, supporta gli endpoint codificati.

Strumenti di crittografia

AWS offre diversi servizi, strumenti e meccanismi di crittografia di dati altamente scalabili, che aiutano a proteggere i dati archiviati ed elaborati in AWS. Per informazioni sulle funzionalità dei servizi AWS e sulla privacy, consultare Funzionalità del servizio AWS per considerazioni sulla privacy[7].

I servizi di crittografia di AWS utilizzano un ampio ventaglio di tecnologie per la codifica e l'archiviazione, progettate per mantenere l'integrità dei dati a riposo o in transito. AWS offre quattro strumenti principali per le operazioni di crittografia.

- ***AWS Key Management Service (AWS KMS)*** è un servizio gestito da AWS che crea e gestisce sia chiavi master sia chiavi dati. AWS KMS è integrato in diversi servizi AWS, per offrire una codifica dati lato server tramite le chiavi KMS dagli account dei clienti. I moduli hardware per la sicurezza KMS (HSMs) sono validati al livello 2 FIPS 140-2.
- ***AWS CloudHSM*** offre HSM validati a livello 3 di FIPS 140-2. Consentono l'archiviazione di una gamma di chiavi di crittografia autogestite, tra cui chiavi master e chiavi dati.
- ***Servizi e strumenti crittografici AWS***
  - ***AWS Encryption SDK*** offre una libreria di crittografia client-side per permettere di implementare la codifica e decodifica di tutti i tipi di dati.
  - ***Amazon DynamoDB Encryption Client*** fornisce una libreria di crittografia client-side per la codifica delle tabelle dati prima che queste vengano inviate a un servizio di database, come Amazon DynamoDB.

AWS Key Management Service

AWS Key Management Service (AWS KMS) è un servizio gestito che facilita la creazione e la gestione delle chiavi di crittografia utilizzate per crittografare i dati. Sfrutta gli Hardware Security Modules (HSMs) per proteggere la sicurezza delle chiavi. AWS KMS si integra con numerosi altri servizi AWS per consentire di proteggere i dati archiviati in tali servizi. AWS

KMS è integrato anche con AWS CloudTrail per fornire i registri dell'utilizzo di tutte le chiavi e consentire di soddisfare i requisiti normativi e di conformità.

Permette di creare, importare e modificare regolarmente le chiavi con la massima semplicità ed è altrettanto facile definire policy di utilizzo e monitorarne l'uso tramite la Console di gestione AWS, il kit SDK o l'interfaccia a riga di comando di AWS.

Le chiavi master in AWS KMS, siano esse importate dall'utente o create da AWS KMS per conto dell'utente e chiamate chiavi master del cliente (CMKs), vengono conservate in archivi estremamente durevoli in formati crittografati, per fare in modo che possano essere usate quando servono. AWS KMS può eseguire la rotazione automatica delle chiavi master create in KMS una volta all'anno senza dover crittografare nuovamente i dati già codificati con la tua chiave master. Non è necessario tenere traccia delle versioni precedenti delle chiavi master perché risulteranno sempre disponibili in AWS KMS per decrittografare i dati precedentemente crittografati.

L'utente può decidere chi ha accesso a ciascuna chiave master in KMS e per quali servizi queste chiavi possono essere utilizzate. Per fare ciò, sono disponibili una serie di controlli accessi, tra cui concessioni e condizioni di policy delle chiavi all'interno delle policy delle chiavi o delle policy IAM. È anche consentito importare chiavi dall'infrastruttura di gestione delle chiavi in uso per impiegarle in KMS.

Ad esempio, la policy in basso sfrutta la condizione kms:ViaService per consentire l'utilizzo di una chiave master del cliente gestita da un cliente per azioni specifiche solo per richieste provenienti da Amazon EC2 o Amazon RDS in una regione specifica (us-west-2) per conto di un utente specifico (ExampleUser).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:ViaService": [
        "ec2.us-west-2.amazonaws.com",
        "rds.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

Figura 7 – Esempio di una policy per Amazon KMS

Integrazione di servizi AWS

AWS KMS è un servizio integrato con molti altri servizi AWS (più di cinquanta nel momento in cui questo documento è stato scritto). Grazie a queste integrazioni, è possibile utilizzare le chiavi master di AWS KMS per crittografare i dati archiviati con tali servizi. Oltre a una chiave master gestita dal cliente, una serie di servizi integrati permettono di usare una chiave master del cliente gestita da AWS creata e gestita per te in modo automatico, ma valida solo per lo specifico servizio per cui è stata creata.

Funzionalità di Audit

Se AWS CloudTrail è abilitato per un account AWS, ogni utilizzo di una chiave archiviata in KMS viene registrato in un file di log che viene trasmesso al bucket di Amazon S3 specificato al momento dell'attivazione di AWS CloudTrail. Le informazioni registrate includono i dettagli relativi all'utente, la data e l'ora di utilizzo della chiave.

Sicurezza

AWS KMS è stato progettato in modo da non consentire a nessuno di accedere alle chiavi master di un cliente. Il servizio è stato sviluppato su sistemi progettati per mantenere al sicuro le chiavi master con tecniche di protezione avanzate, ad esempio salvando su disco solo chiavi master crittografate, disattivandone l'archiviazione in memoria e selezionando i sistemi che possono accedere all'host che le utilizza. L'accesso al software di aggiornamento viene monitorato mediante un processo di controllo multilaterale che viene tenuto sotto controllo e verificato da un gruppo indipendente interno di Amazon.

Per ulteriori informazioni su AWS KMS, consultare il whitepaper AWS Key Management Service.

AWS CloudHSM

Il servizio AWS CloudHSM aiuta a soddisfare i requisiti di conformità aziendali, contrattuali e normativi riguardanti la sicurezza dei dati utilizzando appliance dedicate HSM (Hardware Security Module) nel cloud AWS. CloudHSM consente di controllare le chiavi di crittografia e le operazioni crittografiche eseguite dall'HSM.

I partner di AWS e AWS Marketplace offrono un'ampia gamma di soluzioni per la protezione dei dati sensibili all'interno della piattaforma AWS. Tuttavia, per applicazioni e dati soggetti a obblighi contrattuali o normativi relativi alla gestione delle chiavi crittografiche, può essere necessaria una protezione aggiuntiva. Fino ad ora, l'unica opzione era quella di memorizzare i dati sensibili (o le chiavi di crittografia che proteggono i dati sensibili) nei data center locali. Ciò composta un possibile impedimento nella migrazione di queste applicazioni nel cloud o un rallentamento notevole delle loro prestazioni. Il servizio AWS CloudHSM consente di proteggere le chiavi crittografiche all'interno di moduli HSM progettati e convalidati secondo gli standard governativi per la

gestione sicura delle chiavi. È possibile generare, archiviare e gestire in modo sicuro le chiavi crittografiche usate per la crittografia dei dati, in modo che il cliente sia l'unico utente autorizzato ad accedervi. AWS CloudHSM aiuta a soddisfare i rigorosi requisiti di gestione delle chiavi senza compromettere le prestazioni dell'applicazione.

Il servizio AWS CloudHSM funziona con Amazon Virtual Private Cloud (Amazon VPC). Il provisioning delle istanze CloudHSM viene effettuato all'interno della VPC con un indirizzo IP specificato dall'utente, fornendo una connettività di rete semplice e privata alle istanze Amazon Elastic Compute Cloud (EC2). Poiché le istanze CloudHSM si trovano vicino alle istanze EC2, il loro utilizzo garantisce una latenza di rete inferiore, migliorando le performance dell'applicazione. AWS fornisce un accesso dedicato ed esclusivo (a tenant singolo) alle istanze CloudHSM, che sono isolate da altri clienti AWS. Disponibile in più regioni e zone di disponibilità, CloudHSM permette di aggiungere un archivio di chiavi sicuro e durevole alle tue applicazioni.

Integrazione con Servizi AWS e applicazioni di Terze Parti

CloudHSM può essere utilizzato con Amazon Redshift, Amazon Relational Database Service (Amazon RDS) per Oracle o applicazioni di terze parti (come ad esempio SafeNet Virtual KeySecure) come radice di attendibilità, Apache (terminazioni SSL) o Microsoft SQL Server (crittografia trasparente dei dati). È anche possibile utilizzare CloudHSM per la scrittura di applicazioni proprie e per continuare a utilizzare le librerie crittografiche standard usate abitualmente, come ad esempio PKCS#11, Java JCA/JCE, Microsoft CAPI e CNG.

Attività di Audit

Per monitorare le modifiche alle risorse o controllare le attività di audit su sicurezza e conformità, è possibile esaminare tutte le chiamate API CloudHSM effettuate dal tuo account tramite AWS CloudTrail. Inoltre, è possibile controllare le operazioni sull'appliance HSM usando o inviando messaggi syslog all'agente di raccolta dei log.

Servizi e strumenti crittografici AWS

AWS offre meccanismi che soddisfano un'ampia gamma di standard di sicurezza che puoi usare per implementare una crittografia che rispetti le migliori pratiche. AWS Encryption SDK[8] è una libreria crittografica client-side disponibile in Java, Python, C, JavaScript e un'interfaccia a riga di comando che supporta Linux, macOS e Windows. AWS Encryption SDK offre opzioni avanzate per la protezione dei dati, tra cui suite di chiavi di algoritmi simmetriche, sicure e autenticate, come 256-bit AES-GCM con chiavi di derivazione e accesso. Poiché è stato specificamente progettato per applicazioni che sfruttano Amazon DynamoDB, il DynamoDB Encryption Client[9] permette agli utenti di proteggere le loro tabelle dati prima che vengano inviate al database. Permette, inoltre, di verificare e decifrare dati quando vengono richiamati. Il client è disponibile in Java e Python.

Infrastruttura Linux DM-Crypt

Dm-crypt è un meccanismo di crittografia Linux a livello di kernel che permette agli utenti di montare un sistema di file crittografati. Montare un file system è un processo che consiste nel collegare un file system a una directory (punto di montaggio), mettendolo a disposizione del sistema operativo. Dopo il montaggio, tutti i file nel file system sono disponibili per le applicazioni senza ulteriori interazioni. Tuttavia, questi file sono crittografati quando vengono archiviati nel disco.

Il device mapper è un'infrastruttura nel kernel Linux 2.6 e 3.x che fornisce un metodo generico per creare layer virtuali di dispositivi a blocchi. La destinazione di crittografia del device mapper fornisce una crittografia trasparente di dispositivi a blocchi usando l'API di crittografia del kernel. La soluzione in questo post prevede l'utilizzo di dm-crypt in combinazione con un file system su supporto disco mappato a un volume logico dal Logical Volume Manager (LVM). L'LVM fornisce gestione di volumi logici per il kernel Linux.

Protezione dati fin dalla progettazione e per impostazione predefinita

AWS riceve una richiesta ogni qualvolta un utente o un'applicazione cerchino di usare la Console di gestione AWS, le API AWS o la CLI AWS. Il servizio AWS riceve la richiesta e esegue una serie di fasi per determinare se la richiesta può essere accettata o rifiutata, secondo una specifica logica di valutazione della policy. Tutte le richieste su AWS vengono automaticamente rifiutate (la policy predefinità è deny). Ciò significa che tutto ciò che non viene esplicitamente autorizzato viene rifiutato. Come migliore pratica, nella definizione delle policy, AWS consiglia di applicare il principio del privilegio minimo, che implica che ogni componente (come utenti, moduli o servizi) deve essere in grado di accedere solo alle risorse necessarie per completare le rispettive attività.

Questo approccio riflette l'articolo 25 del GDPR, che stabilisce che il titolare del trattamento "mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento."

AWS fornisce strumenti per implementare l'infrastruttura come codice, che è un potente meccanismo per includere la sicurezza già dalle prime fasi di progettazione di un'architettura. AWS CloudFormation offre un linguaggio comune per descrivere e permettere il provisioning di tutte le risorse delle infrastrutture, incluse le policy e i processi di sicurezza. Grazie a questi strumenti e queste pratiche, la sicurezza entra a far parte del codice e può essere aggiornata, monitorata e modificata (con un sistema di versioning), a seconda delle esigenze dell'organizzazione. Ciò favorisce un approccio di protezione dei dati fin dalla progettazione, in quanto i processi e le policy di sicurezza

possono essere incluse nella definizione dell'architettura oltre a poter essere monitorati in maniera continuata da misure di sicurezza nell'organizzazione.

Il supporto di AWS

Area	*Descrizione*	*Servizi e strumenti AWS*
Solido framework di conformità	Può essere necessario includere nelle misure tecniche e organizzative appropriate "la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione su base continuativa".	SOC 1 / SSAE 16 / ISAE 3402 (precedentemente SAS 70) / SOC 2 / SOC 3 PCI DSS Livello 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Cloud Computing Compliance Controls Catalog (C5)
Controllo dell'accesso ai dati	Il titolare del trattamento "[deve mettere] in atto misure tecniche e organizzative adeguate per garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari per ciascuna finalità specifica del trattamento."	 AWS Identity and Access Management (IAM)  Amazon Cognito  AWS WAF  AWS CloudFormation  AWS Systems Manager
Monitoraggio e logging	"Ogni titolare del trattamento e, ove applicabile, il suo rappresentante devono tenere un registro delle attività di trattamento svolte sotto la propria responsabilità".	 AWS CloudTrail  AWS Config  Amazon CloudWatch  AWS Control Tower  Amazon GuardDuty  AWS Security Hub
Protezione dei dati in AWS	Le organizzazioni devono "[mettere] in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio che comprendono [...] la pseudonimizzazione e la cifratura dei dati personali".	 AWS Tools and SDKs  AWS CloudHSM  AWS Key Management Service

Collaboratori

Hanno collaborato alla stesura di questo documento:

- Tim Anderson, Technical Industry Specialist, Amazon Web Services
- Carmela Gambardella, Public Sector Solutions Architect, Amazon Web Services
- Giuseppe Russo, Security Assurance Manager, Amazon Web Services
- Marta Taggart, Senior Program Manager, Amazon Web Services

Revisioni del documento

Data	*Descrizione*
Ottobre 2019	Aggiornato per inserire i nuovi servizi AWS.
Settembre 2018	Aggiornamenti di minore entità.
Novembre 2017	Prima pubblicazione

Notes

[1] https://ec.europa.eu/info/law/law-topic/data-protection_it

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[3] https://aws.amazon.com/compliance/programs/

[4] https://cispe.cloud/

[5] https://docs.aws.amazon.com/general/latest/gr/rande-manage.html

[6] https://aws.amazon.com/solutions/aws-landing-zone/

[7] https://aws.amazon.com/compliance/data-privacy/service-capabilities/

[8] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-encrypt.html

[9] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-ddb-client.html