Conformità al regolamento generale sulla protezione dei dati in AWS

Novembre 2017

Note

Il presente documento è fornito a solo scopo informativo. In esso sono illustrate le attuali offerte di prodotti e le prassi di AWS alla data di pubblicazione del documento, offerte che sono soggette a modifica senza preavviso. È responsabilità dei clienti effettuare una propria valutazione indipendente delle informazioni contenute nel presente documento e dell'uso dei prodotti o dei servizi di AWS, ciascuno dei quali viene fornito "così com'è", senza garanzie di alcun tipo, né esplicite né implicite. Il presente documento non dà origine a garanzie, rappresentazioni, impegni contrattuali, condizioni o assicurazioni da parte di AWS, delle sue società affiliate, dei suoi fornitori o dei licenzianti. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica qualsivoglia contratto tra AWS e i suoi clienti.

Indice

Regolamento generale sulla protezione dei dati: Panoramica 1

Modifiche introdotte dal GDPR nelle organizzazioni che operano nell'UE 1

Come preparare AWS al GDPR? 1

Il codice di condotta CISPE 2

Controlli sugli accessi ai dati 3

Monitoraggio e registrazione 5

Protezione dei dati in AWS 7

Framework e standard di sicurezza di conformità rigorosi 14

Modello di responsabilità condivisa della sicurezza 15

Responsabilità AWS sulla sicurezza 15

Responsabilità del cliente per la sicurezza 16

Programma Compliance di AWS 17

Cloud Computing Compliance Controls Catalog (C5 – schema tedesco di attestati riconosciuti dal governo) 18

Revisioni del documento 19

Sintesi

Il Regolamento generale sulla protezione dei dati (il "GDPR") entrerà in vigore il 25 maggio 2018. AWS offre servizi e risorse che ti aiuteranno a rispettare i requisiti del GDPR eventualmente applicabili alle tue operazioni. Tra i servizi e le risorse sono inclusi la conformità di AWS al codice di condotta CISPE, i controlli di accesso ai dati granulari, gli strumenti di monitoraggio e registrazione, la crittografia, la gestione delle chiavi, la capacità di audit, la conformità a standard di sicurezza IT e gli attestati C5 rilasciati ad AWS.

Regolamento generale sulla protezione dei dati: Panoramica

Il Regolamento generale sulla protezione dei dati (nel prosieguo, GDPR) è una nuova normativa europea in materia privacy che entrerà in vigore il 25 maggio 2018. Lo scopo del GDPR è armonizzare le normative in materia di protezione dei dati all'interno dell'Unione europea (UE) mediante l'adozione di un'unica legge che avrà valore vincolante in ogni Stato membro.

Il GDPR si applica a tutte le organizzazioni che hanno sede nell'UE o che offrono beni o servizi ai cittadini comunitari in relazione al trattamento di "dati personali" di residenti dell'UE. Per "dati personali" si intendono informazioni, di qualunque tipo, relative a una persona fisica identificata o identificabile.

Il GDPR sostituirà l'attuale Direttiva dell'UE sulla protezione dei dati (Direttiva europea 95/46/CE). Dal 25 maggio 2018, l'attuale Direttiva dell'UE sulla protezione dei dati e le leggi ad essa relative cesseranno di essere efficaci.

Modifiche introdotte dal GDPR nelle organizzazioni che operano nell'UE

Uno degli aspetti principali del GDPR è l'intento di uniformare le modalità di trattamento, uso e scambio sicuro dei dati personali in tutti gli Stati membri. Le organizzazioni dovranno dimostrare, su base continuativa, la sicurezza dei dati trattati e la conformità al GDPR, implementando e rivedendo regolarmente misure tecniche e organizzative, oltre ai requisiti di conformità. Sarà possibile per le autorità di vigilanza imporre sanzioni fino a 20 milioni di euro o corrispondenti al 4% del volume di affari globale annuo, se superiore.

Come preparare AWS al GDPR?

Gli esperti in materia di conformità, protezione dei dati e sicurezza di AWS hanno lavorato fianco a fianco con i nostri clienti in tutto il mondo per rispondere alle loro domande e aiutarli a prepararsi ad affrontare carichi di lavoro nel cloud AWS dopo l'entrata in vigore del GDPR. Questi team hanno anche riesaminato tutte le azioni già intraprese da AWS per assicurarne la conformità con i requisiti del GDPR.

> Possiamo confermare che tutti i servizi AWS saranno conformi al GDPR quando entrerà in vigore nel maggio 2018.

Ai sensi dell'articolo 32, il titolare del trattamento e il responsabile del trattamento devono mettere "in atto misure tecniche e organizzative" 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 fornisce suggerimenti specifici sul tipo di azioni di sicurezza richieste, che includono:

- La pseudonimizzazione e la cifratura dei dati personali.
- La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
- La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
- Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il codice di condotta CISPE

Il GDPR prevede l'approvazione di codici di condotta per aiutare i titolari e i responsabili del trattamento a dimostrare la conformità e la best practice. Uno di questi codici, in attesa dell'approvazione ufficiale, è il codice di condotta del CISPE per i fornitori di servizi infrastrutturali cloud (il "Codice"). Il Codice rassicura i clienti perché dimostra che il loro fornitore di soluzioni adotta standard di protezione dati idonei e conformi al GDPR.

Ecco alcuni dei vantaggi principali:

- **Determinazione delle responsabilità in materia di protezione dei dati.** Il Codice di condotta illustra il ruolo del fornitore e del cliente ai sensi del GDPR, in particolare nel contesto dei servizi infrastrutturali cloud.

- **Il Codice di condotta definisce i principi che i fornitori sono tenuti a rispettare.** Definisce inoltre i principi fondamentali del GDPR relativi alle attività che i fornitori devono svolgere e agli impegni che si devono assumere per consentire ai clienti di essere conformi. I clienti possono fare affidamento sui vantaggi concreti offerti dalla conformità e dalle strategie di protezione dei dati.
- **Il Codice di condotta offre ai clienti le informazioni sulla sicurezza necessarie per prendere decisioni in merito alla conformità**. Richiede ai fornitori di essere trasparenti in merito alle procedure adottate per garantire il rispetto degli impegni nell'ambito della sicurezza. Tali procedure prevedono, a titolo esemplificativo, le notifiche di violazioni dei dati, la cancellazione dei dati, l'affidamento del processo di elaborazione a terze parti, nonché le richieste delle autorità governative di competenza e delle forze dell'ordine. I clienti possono utilizzare queste informazioni per acquisire piena consapevolezza degli elevati livelli di sicurezza forniti.

Il 13 febbraio 2017 AWS ha dichiarato che Amazon Elastic Compute Cloud (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) sono pienamente conformi al Codice (vedere).https://cispe.cloud/publicregister Ciò garantisce ai nostri clienti l'ulteriore assicurazione che i controlli cui sono sottoposti i loro dati siano condotti in un ambiente protetto, sicuro e conforme quando utilizzano AWS. La conformità al Codice si aggiunge alla lunga serie di certificazioni e accreditamenti internazionalmente riconosciuti già in possesso di AWS, quali ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2 e SOC 3, PCI DSS Livello 1 e molti altri.

Controlli sugli accessi 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 di controllo degli accessi di AWS contribuiscono a garantire la conformità al presente requisito,

consentendo l'accesso alle risorse AWS e ai dati dei clienti esclusivamente alle applicazioni, agli amministratori e agli utenti autorizzati:

- **Accesso con un livello di granularità fine a oggetti AWS in bucket S3/SQS/SNS e altri –** Puoi concedere permessi diversi a persone diverse per risorse diverse. Ad esempio, è possibile concedere ad alcuni utenti di avere accesso completo ad Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift, e altri servizi AWS. Agli altri utenti puoi consentire l'accesso in modalità di sola lettura limitatamente ad alcuni bucket S3, l'amministrazione solo di alcune istanze EC2 o l'accesso alle tue informazioni di fatturazione, e nient'altro.
- **Autenticazione a più fattori o MFA (Multi-Factor Authentication) –** È possibile aggiungere al proprio account e agli utenti individuali un'autenticazione a due fattori per aumentare il livello di sicurezza. Per utilizzare l'account, con MFA è necessario che tu o gli utenti forniate non solo una password o la chiave di accesso, ma anche un codice proveniente da un dispositivo appositamente configurato.
- **Autenticazione delle richieste API –** Puoi utilizzare le caratteristiche IAM per fornire in tutta sicurezza alle applicazioni eseguite su istanze EC2 le credenziali necessarie per accedere ad altre risorse AWS come bucket S3, RDS o database DynamoDB.
- **Restrizioni geografiche –** Puoi utilizzare restrizioni geografiche, note anche come geoblocking, per impedire a utenti in specifiche posizioni geografiche di accedere a contenuti diffusi attraverso una distribuzione Web CloudFront. Per utilizzare le restrizioni geografiche, sono disponibili due opzioni:
    - **Uso della caratteristica Restrizione geografica CloudFront.** Usa questa opzione per limitare l'accesso a tutti i file associati a una distribuzione e per limitare l'accesso a livello nazionale.
    - **Uso del servizio di geolocalizzazione di terze parti.** Con questa opzione puoi limitare l'accesso a un sottoinsieme di file associati a una distribuzione e a un livello di granularità più fine rispetto a quello nazionale.
- **Token di accesso temporaneo tramite STS –** Puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza

provvisorie in grado di controllare l'accesso alle risorse AWS e fornirle a utenti affidabili. Le credenziali di sicurezza provvisorie funzionano in modo quasi identico rispetto alle credenziali delle chiavi di accesso a lungo termine che gli utenti IAM possono utilizzare, tranne per le differenze seguenti:

- **Come dice il nome, le credenziali di sicurezza provvisorie hanno vita breve.** Possono essere configurate per durare da pochi minuti ad alcune ore. Le credenziali scadute non vengono più riconosciute da AWS, che nega inoltre qualsiasi tipo di accesso da richieste API effettuate con esse.
- **Le credenziali di sicurezza provvisorie non vengono memorizzate dall'utente ma sono generate dinamicamente e messe a disposizione dell'utente su richiesta.** Alla scadenza delle credenziali (o anche prima), l'utente può richiederne di nuove, a condizione che disponga ancora delle autorizzazioni per farlo.

Queste differenze producono i seguenti vantaggi nell'utilizzo delle credenziali provvisorie:

- Le credenziali di sicurezza AWS a lungo termine non potranno essere distribuite con un'applicazione né incorporate in essa.
- È possibile offrire l'accesso alle risorse AWS senza la necessità di definire una AWS Identity per gli utenti. Le credenziali provvisorie costituiscono la base dei ruoli e della federazione delle identità.
- Essendo caratterizzate da un ciclo di vita limitato, quando non servono più le credenziali di sicurezza non possono essere modificate o esplicitamente revocate. Dopo la loro scadenza, le credenziali di sicurezza provvisorie non possono essere riutilizzate. Puoi specificare la durata della validità delle credenziali, fino al limite massimo.

Monitoraggio e registrazione

Il GDPR prevede che "[o]gni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità." Il presente articolo include anche i dettagli delle informazioni da registrare. In altre parole, il GDPR prevede il monitoraggio del trattamento dei dati PII. Gli obblighi di notifiche tempestive delle violazioni

richiedono inoltre che gli incidenti vengano rilevati quasi in tempo reale. Per aiutarti a essere conforme rispetto a tali obblighi, AWS offre diversi servizi di monitoraggio e registrazione di log:

- **Gestione e configurazione delle risorse con AWS Config** – AWS Config offre una dettagliata panoramica della configurazione delle risorse AWS nell'account AWS. Sono inclusi il modo in cui le risorse sono correlate e in cui sono state configurate in passato, per permetterti di registrare il modo in cui le configurazioni e relazioni cambiano nel tempo.

  Una risorsa AWS è un'entità con cui è possibile lavorare in AWS, ad esempio un'istanza Amazon Elastic Compute Cloud (EC2), un volume Amazon Elastic Block Store (EBS), un gruppo di sicurezza o un Amazon Virtual Private Cloud (VPC). Per un elenco completo delle risorse AWS supportate da AWS Config, vedere Tipi di risorse AWS supportate.

  AWS Config offre le seguenti possibilità:

  - Valutare le configurazioni di una determinata risorsa AWS per le impostazioni desiderate.
  - Ottenere uno snapshot delle attuali configurazioni delle risorse supportate associate all'account AWS.
  - Recuperare le configurazioni di almeno una delle risorse esistenti nell'account.
  - Recuperare lo storico delle configurazioni di almeno una delle risorse.
  - Ricevere una notifica ogni volta che una risorsa viene creata, modificata o eliminata.
  - Visualizzare le relazioni tra le risorse. Ad esempio, si potrebbero trovare tutte le risorse che utilizzano un particolare gruppo di sicurezza.
- **Audit di conformità e analisi di sicurezza con AWS CloudTrail** – Con AWS CloudTrail è possibile monitorare le distribuzioni AWS nel cloud, generando lo storico delle chiamate API AWS per il tuo account, fra cui le chiamate API effettuate tramite la Console di gestione AWS, gli SDK AWS, gli strumenti a riga di comando e i servizi AWS di livello

superiore. Puoi inoltre 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 percorsi per la tua organizzazione, verificare lo stato dei percorsi e controllare come gli amministratori attivano o disattivano la generazione di log CloudTrail.

- **Identificazione dei problemi di configurazione tramite AWS Trusted Advisor –** La registrazione di log offre la possibilità di distribuire log dettagliati a un bucket S3. Un log degli accessi contiene i dettagli della richiesta, quali tipo di richiesta, risorse specificate nella richiesta e ora e data in cui la richiesta è stata elaborata. Per ulteriori informazioni sui contenuti di un log, vedere Server Access Log Format[1] nella Amazon Simple Storage Service Developer Guide.
- I log di accesso al server sono utili per numerose applicazioni, perché offrono ai proprietari dei bucket informazioni sulla natura delle richieste effettuate dai client che non sono sotto il loro controllo. Per impostazione predefinita, Amazon S3 non raccoglie i log di accesso al server, ma distribuisce i log di accesso al bucket su base oraria se viene abilitata la registrazione di log.
- Registrazione di log con un livello di granularità fine degli accessi a oggetti 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.
- Filtro e monitoraggio degli accessi HTTP alle applicazioni con funzioni WAF in CloudFront.

Protezione dei dati in AWS

Il 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 (...)." Le organizzazioni devono inoltre tutelarsi affinché i dati personali non vengano divulgati o non vi si acceda senza autorizzazione. Infine, nel caso in cui si sia verificata una violazione dei dati personali che è probabile presenti un

elevato rischio per i diritti e le libertà delle persone fisiche, sebbene i titolari abbiano posto in essere "misure di sicurezza tecniche e organizzative (...) quali la cifratura", non è necessario che i titolari notifichino i dati in questione oggetto della violazione, potendo in questo modo evitare i costi amministrativi e i danni alla reputazione. AWS propone numerosi meccanismi altamente scalabili e sicuri di crittografia dei dati per aiutare i clienti a proteggere i dati archiviati ed elaborati in AWS:

- **Crittografia dei tuoi dati inattivi con AES256 (EBS/S3/Glacier/RDS) –** La crittografia dei dati inattivi[2] è imprescindibile per garantire la conformità ai requisiti normativi, assicurando che i dati sensibili salvati su disco non possano essere letti da nessun utente o applicazione senza una chiave valida. AWS mette a disposizione opzioni di dati inattivi e la gestione delle chiavi a supporto del processo di crittografia. Ad esempio, è possibile crittografare i volumi di Amazon EBS e configurare i bucket di Amazon S3 per la crittografia lato server (SSE) usando la crittografia AES-256. Inoltre, Amazon RDS supporta la crittografia TDE (Transparent Data Encryption).

  Lo storage dell'istanza offre storage temporaneo a livello di blocco per le istanze Amazon EC2. Questo storage è situato su dischi collegati fisicamente a un computer host. Lo storage dell'istanza è perfetto per uno storage temporaneo di informazioni che cambiano di continuo, quali buffer, cache e dati da zero. Per impostazione predefinita, i file archiviati su questi dischi non vengono crittografati.

  - **Crittografia di dischi e file system** – Puoi utilizzare due metodi per crittografare i file su instance store. Il primo metodo è la crittografia del disco, che si effettua sull'intero disco o su un blocco al suo interno usando almeno una chiave di crittografia. La crittografia 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. La crittografia di File System, ad esempio, è un'estensione Microsoft del file system NTFS (New Technology File System) del sistema operativo Windows NT che prevede la crittografia del disco.

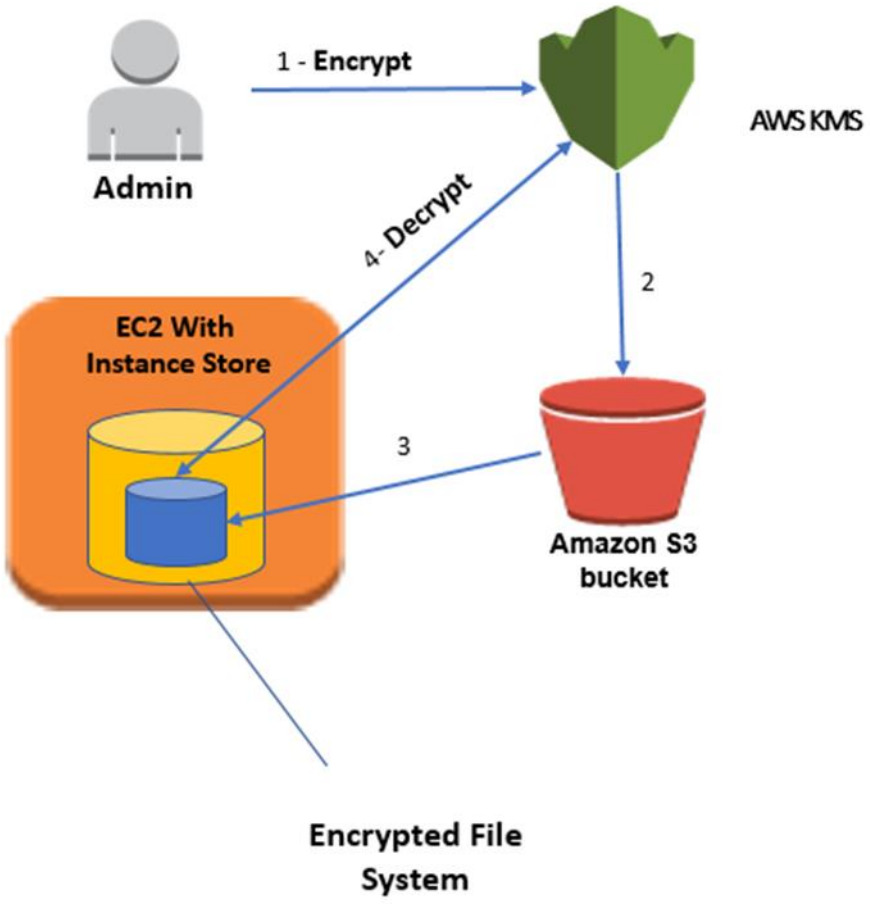
    Il secondo metodo consiste nella crittografia a livello di file system. Vengono crittografati i file e le directory, non il disco o la partizione

per intero. La crittografia a livello file system opera su file system ed è portabile da un sistema operativo all'altro.

- **Infrastruttura Linux dm-crypt** – Il dm-crypt è un meccanismo di crittografia a livello di kernel Linux che consente agli utenti di montare un file system crittografato. Montare un file system significa collegarlo 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; una volta archiviati su disco questi file vengono tuttavia crittografati.

  Il mappatore di dispositivo è un'infrastruttura nel kernel Linux 2.6 e 3.x che permette di creare livelli virtuali di dispositivi a blocchi in modo generico. Il crypt target del mappatore di dispositivo permette di eseguire una crittografia trasparente dei 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). LVM esegue la gestione del volume logico per il kernel Linux.

- **Panoramica sull'architettura** – Il seguente diagramma architettonico di alto livello illustra la soluzione proposta per abilitare la crittografia EC2 instance store.



1. L'amministratore esegue la crittografia di una password segreta utilizzando KMS. La password crittografata viene archiviata in un file.
2. L'amministratore trasferisce il file contenente la password crittografata in un bucket S3.
3. All'avvio dell'istanza, il file crittografato viene copiato su un disco interno.
4. L'istanza EC2 quindi decrittografa il file utilizzando KMS e ripristina la password non crittografata. La password viene utilizzata per configurare il file system crittografato di Linux con LUKS. Una volta archiviati su disco, tutti i dati scritti nel file

system crittografato vengono a loro volta crittografati mediante un algoritmo AES-256.

- **Gestione delle chiavi in modo centralizzato (per regione)** – AWS Key Management Service (KMS) è un servizio gestito che semplifica la creazione e il controllo delle chiavi di crittografia usate per crittografare i dati e utilizza moduli di sicurezza hardware o HSM (Hardware Security Module) per proteggere le chiavi. AWS Key Management Service si integra con numerosi altri servizi AWS per consentirti di proteggere i dati memorizzati assieme a tali servizi. AWS Key Management Service 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.
    - **Gestione centralizzata delle chiavi** – AWS Key Management Service garantisce un controllo centralizzato di tutte le chiavi di crittografia. È possibile creare, importare e modificare regolarmente le chiavi con la massima semplicità; è sufficiente definire delle policy di utilizzo e monitorarne l'uso tramite la Console di gestione AWS, kit SDK o interfaccia a riga di comando di AWS. Le chiavi master in KMS, sia quelle importate sia quelle create da KMS, vengono immagazzinate in storage crittografati estremamente durevoli, per semplificarne il recupero, quando necessario. Puoi impostare KMS in modo che esegua la rotazione automatica delle chiavi master create in KMS una volta all'anno senza dover crittografare nuovamente i dati già codificati in base alla chiave master. Non dovrai tenere traccia delle versioni precedenti delle chiavi master perché risulteranno sempre disponibili in KMS per decrittografare i dati precedentemente crittografati. Puoi creare nuove chiavi master e controllare chi ha accesso a tali chiavi e con quali servizi puoi utilizzarle in qualsiasi momento. Potrai anche importare chiavi dall'infrastruttura di gestione delle chiavi in uso per impiegarle in KMS.
    - **Integrazione con i servizi AWS** – AWS Key Management Service è integrato con numerosi altri servizi AWS. Grazie a questa integrazione, puoi utilizzare le chiavi master di AWS KMS per crittografare i dati memorizzati con i servizi interessati. Puoi usare una chiave master predefinita creata automaticamente e utilizzabile all'interno del servizio integrato o selezionare una chiave master

personalizzata creata in KMS o importata dall'infrastruttura di gestione delle chiavi in uso e per la quale disponi del permesso di utilizzo.

- **Capacità di audit** – Se hai abilitato AWS CloudTrail[3] per il tuo account AWS, ogni utilizzo di una chiave memorizzata 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 chiave, nonché la data e l'ora di utilizzo di tale chiave.
- **Scalabilità, durabilità ed elevata disponibilità** – AWS Key Management Service è un servizio gestito. A mano a mano che aumentano le tue esigenze di utilizzo delle chiavi di crittografia di AWS KMS, non sarai costretto ad acquistare elementi aggiuntivi per la tua infrastruttura per la gestione delle chiavi. AWS KMS ricalibra automaticamente le risorse in base alle esigenze relative alle chiavi di crittografia.

  Le chiavi master create da AWS KMS o importate non possono essere esportate. AWS KMS memorizza più copie delle versioni crittografate delle chiavi in sistemi caratterizzati da una durabilità pari al 99,999999999% per garantire la costante disponibilità delle chiavi quando è necessario. Se importi chiavi in KMS, consigliamo di conservarne una copia in un percorso sicuro per poterle eventualmente reimportare in qualsiasi momento.

  AWS KMS è distribuito in più zone di disponibilità all'interno di una regione AWS a garanzia dell'elevata disponibilità delle chiavi di crittografia.
- **Sicurezza** – AWS KMS è stato progettato in modo da non consentire a nessuno di accedere alle tue chiavi master. 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 e utilizzarle. 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 sul funzionamento di AWS KMS, consulta il whitepaper relativo a AWS Key Management Service[4].

- **Tunnel IPsec in AWS con i gateway VPN** – Amazon VPC consente di allestire una sezione logicamente isolata del cloud di Amazon Web Services (AWS) dove è possibile avviare risorse AWS in una rete virtuale definita dal cliente. Quest'ultimo ha il controllo completo dell'ambiente di rete virtuale, che include la selezione di una gamma di indirizzi IP, la creazione di subnet e la configurazione di tabelle di routing e gateway di rete. Inoltre, potrai creare una connessione VPN hardware tra il tuo data center aziendale e la VPC per utilizzare il cloud AWS come estensione del data center aziendale.

  Personalizzare la configurazione di rete di Amazon VPC è molto semplice. Ad esempio, è possibile creare una sottorete pubblica per i server Web dotata di accesso a Internet e collocare i sistemi back-end quali database o server di applicazioni in una sottorete privata senza accesso a Internet. Grazie ai vari livelli di sicurezza disponibili, come i gruppi di sicurezza e le liste di controllo degli accessi di rete, è possibile controllare l'accesso alle istanze di Amazon EC2 in ciascuna sottorete.

- **Moduli HSM dedicati nel cloud con AWS CloudHSM** – Il servizio AWS CloudHSM consente di soddisfare i requisiti di conformità aziendali, contrattuali e normativi riguardanti la sicurezza dei dati utilizzando appliance HSM (Hardware Security Module) all'interno del cloud AWS. CloudHSM consente di controllare le chiavi di crittografia e le operazioni crittografiche eseguite dal modulo di protezione hardware (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, quando si ha a che fare con applicazioni e dati soggetti a rigorosi requisiti contrattuali o normativi per la gestione delle chiavi crittografiche, talvolta è necessaria una protezione aggiuntiva. Fino a oggi l'unica opzione prevedeva l'archiviazione di dati sensibili (o delle chiavi di crittografia a protezione dei dati sensibili) nei data center locali. Purtroppo, questo ostacolava la migrazione di queste applicazioni nel cloud oppure ne rallentava notevolmente le prestazioni. Il servizio AWS CloudHSM consente di proteggere le chiavi di crittografia all'interno dei moduli di protezione hardware progettati e convalidati dagli 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 siano accessibili solo all'utente. AWS CloudHSM consente di soddisfare i rigorosi requisiti di gestione delle chiavi senza compromettere in alcun modo le prestazioni dell'applicazione.

Il servizio AWS CloudHSM funziona con Amazon Virtual Private Cloud (VPC). Il provisioning delle istanze CloudHSM viene eseguito all'interno di VPC con l'indirizzo IP specificato; questo garantisce in modo semplice una connettività di rete privata per le istanze Amazon Elastic Compute Cloud (EC2). Il fatto che le istanze CloudHSM si trovino accanto alle istanze EC2 riduce la latenza di rete e migliora le prestazioni dell'applicazione. AWS offre accesso dedicato ed esclusivo con tenant singolo alle istanze CloudHSM, isolate da altri clienti AWS. AWS CloudHSM è disponibile in più regioni e zone di disponibilità garantendo alle applicazioni l'archiviazione sicura e durevole delle chiavi.

- **Integrazione** – CloudHSM può essere utilizzato con Amazon Redshift, Amazon Relational Database Service (RDS) 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 continuare a utilizzare le librerie crittografiche standard usate abitualmente, come ad esempio PKCS#11, Java JCA/JCE, Microsoft CAPI e CNG.
- **Controlli** - Per tracciare le modifiche delle risorse o controllare le attività per scopi di sicurezza e conformità, è possibile rivedere tutte le chiamate API CloudHSM eseguite dall'account tramite CloudTrail. Inoltre, è possibile controllare le operazioni nell'appliance HSM usando o inviando messaggi registro syslog all'agente di raccolta.

Framework e standard di sicurezza di conformità rigorosi

Conformemente al GDPR, è possibile che le misure tecniche organizzative adeguate debbano includere "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di

trattamento" oltre a processi affidabili di ripristino, controlli e gestione dei rischi. AWS offre un rigoroso framework di conformità e avanzati standard di sicurezza.

Modello di responsabilità condivisa della sicurezza

Prima di analizzare nel dettaglio la modalità con cui AWS protegge i dati, è necessario parlare della leggera differenza tra la sicurezza nel cloud e la sicurezza nei data center locali. Nel momento in cui trasferisci sistemi informatici e dati al cloud, le responsabilità sulla sicurezza vengono condivise tra te e il tuo fornitore di servizi cloud. In questo caso, AWS ha la responsabilità di proteggere l'infrastruttura che supporta il cloud, mentre tu sei responsabile di tutto ciò che viene trasferito o collegato al cloud. Questo modello di responsabilità condivisa della sicurezza è in grado di ridurre il tuo carico operativo sotto vari aspetti e in alcuni casi può persino migliorare la sicurezza predefinita senza richiede alcuna azione aggiuntiva.

Responsabilità AWS sulla sicurezza

Amazon Web Services si occupa di proteggere l'infrastruttura globale su cui vengono eseguiti tutti i servizi offerti nel cloud AWS. L'infrastruttura è composta dai componenti hardware e software, le reti e le strutture che eseguono i servizi AWS. La protezione di questa infrastruttura è la priorità numero uno di AWS e, sebbene tu non possa visitare i nostri data center o uffici per scoprire in prima persona questo livello di protezione, possiamo trasmetterti report di revisori di terze parti che attestano la nostra conformità rispetto a un'ampia gamma di regolamenti e standard di sicurezza informatici. Ulteriori informazioni sono disponibili all'indirizzo https://aws.amazon.com/compliance/.

Si noti che oltre a tutelare questa infrastruttura globale, AWS è anche responsabile della configurazione di sicurezza dei suoi prodotti considerati come servizi gestiti. Tra questi tipi di servizi figurano, ad esempio, Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces e molti altri. Tali servizi offrono la scalabilità e la flessibilità proprie delle risorse basate sul cloud con l'ulteriore vantaggio di essere gestiti. Per questi servizi, AWS gestirà attività di sicurezza di base, come l'applicazione di patch al sistema operativo guest (OS) e ai guest database, la configurazione del firewall e il disaster recovery. Per la maggior parte di questi

servizi gestiti, tutto ciò che devi fare è configurare i controlli sugli accessi logici per le risorse e proteggere le tue credenziali dell'account. In alcuni casi potrebbero rendersi necessarie attività aggiuntive, quali la configurazione degli account utente dei database, ma nel complesso l'opera di configurazione viene assolta dal servizio.

Responsabilità del cliente per la sicurezza

Con il cloud AWS è possibile effettuare il provisioning di dispositivi di storage, database, desktop e server virtuali nel giro di pochi minuti anziché settimane. Puoi inoltre utilizzare gli strumenti di analisi e flussi di lavoro basati sul cloud per elaborare i dati secondo necessità, per poi archiviarli nei tuoi data center o nel cloud. L'entità del lavoro di configurazione che dovrai svolgere nell'ambito delle tue responsabilità in materia di sicurezza dipenderà dai servizi AWS di cui deciderai di usufruire.

I prodotti AWS che rientrano nella sperimentata categoria IaaS (Infrastructure as a Service), ad esempio, servizi come Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC) e Amazon S3, sono completamente sotto il controllo del cliente e richiedono che sia lui ad eseguire tutte le necessarie attività di configurazione e gestione della sicurezza. Per quanto riguarda le istanze EC2, ad esempio, sarà tua la responsabilità della gestione del sistema operativo guest (inclusi aggiornamenti e patch di sicurezza), di qualsiasi software applicativo o utilità da installati sulle istanze e della configurazione del firewall fornito da AWS (chiamato gruppo di sicurezza) in ogni istanza. Si tratta sostanzialmente delle stesse attività di sicurezza che sei solito eseguire indipendentemente dalla posizione in cui si trovano i tuoi server.

I servizi gestiti AWS come Amazon RDS o Amazon Redshift mettono a disposizione tutte le risorse necessarie per eseguire un'attività specifica, senza tuttavia il lavoro di configurazione generalmente associato ad esse. Grazie ai servizi gestiti non ti devi preoccupare del lancio o della manutenzione delle istanze, dell'applicazione di patch ai database o sistemi operativi guest, né della replica dei database, perché AWS provvede a tutto ciò per conto tuo. Come per tutti i servizi, tuttavia, sei tenuto a proteggere le tue credenziali dell'account AWS e configurare i singoli account utente con Amazon Identity and Access Management (IAM) in modo che tutti i tuoi utenti siano in possesso delle proprie credenziali e diventi possibile implementare la separazione dei compiti. Consigliamo inoltre di utilizzare l'autenticazione multi-fattore (MFA, multi-

factor authentication) per ogni account, con conseguente adozione della protezione SSL/TLS per comunicare con le risorse AWS, e la configurazione della registrazione delle attività utente/API con AWS CloudTrail. Per maggiori informazioni sulle ulteriori misure che si possono attuare, rinviamo alla lettura del whitepaper sulle best practice di sicurezza di AWS e della pagina Web sulle risorse di sicurezza di AWS.

Programma Compliance di AWS

Conformità di Amazon Web Services consente di conoscere i solidi sistemi di controllo messi in atto da AWS per proteggere i dati nel cloud. Poiché i sistemi sono basati sull'infrastruttura cloud di AWS, le responsabilità di conformità saranno condivise. Mettendo a stretto contatto servizi basati su governance compatibili con sistemi di controllo e standard di conformità e di audit, gli strumenti per la conformità di AWS si basano su programmi tradizionali che consentono di affermarsi e lavorare nell'ambiente protetto di AWS. L'infrastruttura IT che AWS fornisce è progettata e gestita secondo le practice di sicurezza e nel rispetto di una serie di standard di sicurezza IT, inclusi:

- SOC 1/SSAE 16/ISAE 3402 (ex SAS70)
- SOC 2
- SOC 3
- FISMA, DIACAP e FedRAMP
- DoD CSM Livelli 1-5
- PCI DSS Livello 1
- ISO 9001, ISO 27001
- ITAR
- FIPS 140-2
- MTCS livello 3

Le caratteristiche di flessibilità e controllo offerte dalla piattaforma AWS permettono di distribuire soluzioni in grado di rispondere a vari standard applicabili a settori specifici, fra cui:

- Criminal Justice Information Services (CJIS)

- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

AWS fornisce ai clienti una vasta gamma di informazioni sull'ambiente di controllo IT, tramite whitepaper, documenti, certificazioni, accreditamenti e altre attestazioni di terze parti. Per ulteriori informazioni è possibile consultare il whitepaper AWS su rischio e compliance disponibile alla pagina http://aws.amazon.com/compliance/.

Cloud Computing Compliance Controls Catalog (C5 – schema tedesco di attestati riconosciuti dal governo)

Cloud Computing Compliance Controls Catalog (C5)[5] è uno schema tedesco di attestati riconosciuti dal governo introdotto in Germania dal Federal Office for Information Security (BSI) per aiutare le organizzazioni a dimostrare la sicurezza a livello operativo rispetto agli attacchi informatici comuni nell'ambito delle Security Recommendations for Cloud Providers[6] del governo tedesco.

L'attestato può essere utilizzato 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 aggiunge controlli aggiuntivi che forniscono informazioni sulla posizione dei dati, il provisioning dei servizi, la sede di giurisdizione, la certificazione esistente, obblighi di divulgazione delle informazioni e una descrizione completa del servizio. Utilizzando queste informazioni, i clienti possono valutare in che modo le normative legali (ad esempio la privacy dei dati), le proprie politiche o l'ambiente delle minacce sono correlati all'utilizzo dei servizi di cloud computing.

Revisioni del documento

Data	Descrizione
Novembre 2017	Prima pubblicazione

Notes

[1] http://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html

[2] https://do.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

[3] https://aws.amazon.com/cloudtrail/

[4] https://do.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf

[5] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/ComplianceControlsCatalogue.pdf;jsessionid=E5F009E49EB2689FAC3705578821BCB6.2_cid286?__blob=publicationFile&v=3

[6] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile&v=2