Whitepaper AWS

Introduzione alla sicurezza di AWS

Introduzione alla sicurezza di AWS: Whitepaper AWS

Table of Contents

Introduzione alla sicurezza di AWS

Data di pubblicazione: 11 novembre 2021 (Revisioni del documento)

Riassunto

Amazon Web Services (AWS) offre una piattaforma di cloud computing scalabile progettata per fornire disponibilità elevata e affidabilità, mettendo a disposizione gli strumenti per la gestione di un'ampia gamma di applicazioni. Per AWS è essenziale non solo proteggere la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati dei clienti, ma anche mantenere la loro fiducia. Questo documento ha lo scopo di fornire un'introduzione all'approccio di AWS alla sicurezza, con informazioni sui controlli nell'ambiente AWS e su alcuni dei prodotti e delle caratteristiche che AWS offre ai clienti per soddisfare gli obiettivi di sicurezza.

Sicurezza dell'infrastruttura AWS

L'infrastruttura AWS è stata progettata per offrire un ambiente di cloud computing tra i più sicuri e flessibili attualmente disponibili. È pensata per fornire una piattaforma estremamente scalabile e affidabile che permette ai clienti di distribuire applicazioni e dati in modo rapido e sicuro.

Questa infrastruttura è creata e gestita non solo nel rispetto degli standard e delle best practice per la sicurezza, ma anche tenendo presenti le esigenze specifiche del cloud. AWS usa controlli ridondanti e su più livelli, convalida e test continui, nonché una sostanziale quantità di automazione per assicurare il monitoraggio e la protezione dell'infrastruttura sottostante 24 ore su 24, 7 giorni su 7. AWS si assicura che questi controlli vengano replicati in ogni nuovo data center o servizio.

Tutti i clienti AWS possono usufruire dei vantaggi di un'architettura di data center e di rete progettata per soddisfare i requisiti degli utenti più esigenti a livello di sicurezza. Ciò significa ottenere un'infrastruttura resiliente progettata per un elevato livello di sicurezza, senza l'esborso di capitale e senza il sovraccarico operativo di un data center tradizionale.

AWS opera in base a un modello di responsabilità condivisa della sicurezza, in cui AWS è responsabile della sicurezza dell'infrastruttura cloud sottostante, mentre l'utente è responsabile della sicurezza dei carichi di lavoro implementati in AWS (Figura 1). In questo modo si ottengono la flessibilità e l'agilità necessarie per implementare la maggior parte dei controlli di sicurezza applicabili per le funzioni aziendali nell'ambiente AWS. È possibile limitare rigorosamente l'accesso agli ambienti che elaborano dati sensibili o distribuire controlli meno rigorosi per le informazioni che si desidera rendere pubbliche.

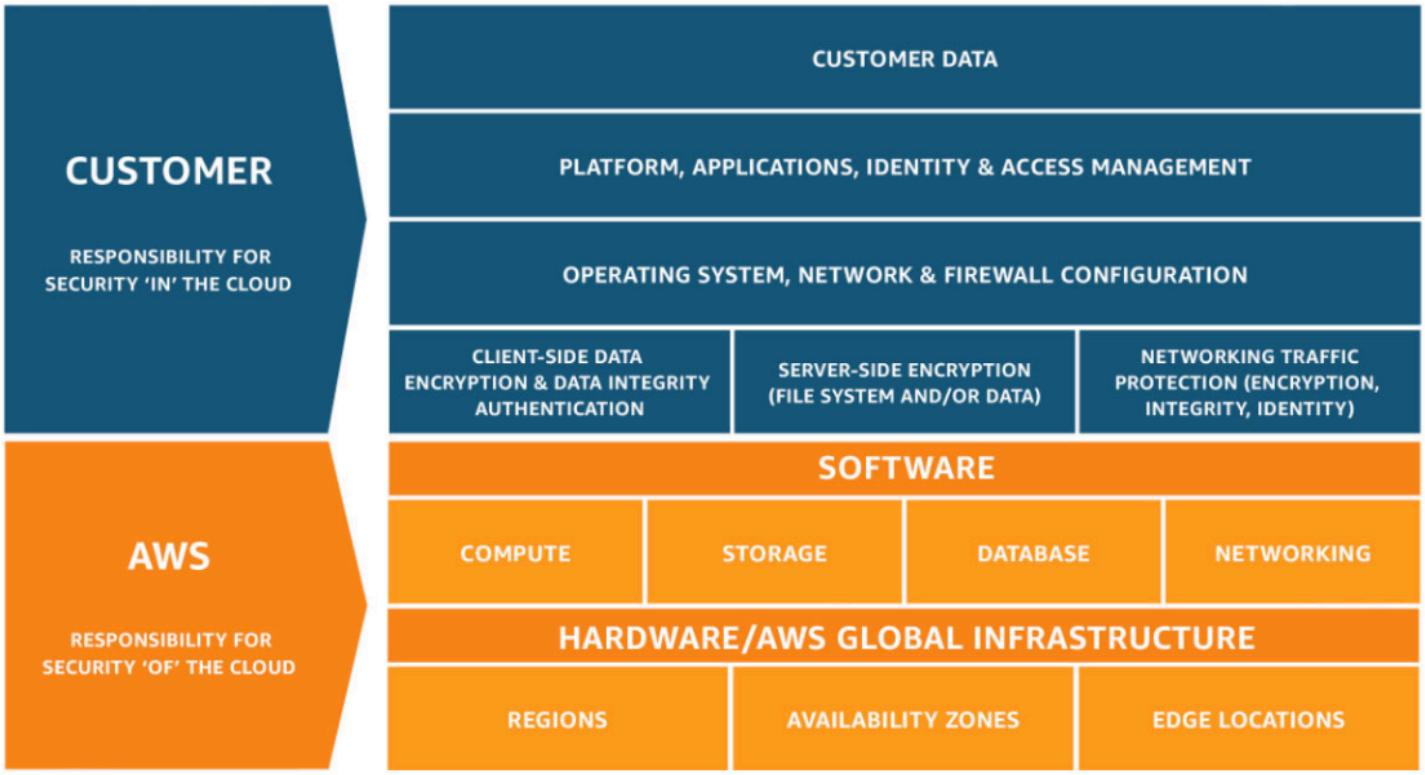

Figura 1: Modello di responsabilità condivisa della sicurezza di AWS

Prodotti e caratteristiche per la sicurezza

AWS e i suoi partner offrono una vasta gamma di strumenti e caratteristiche che aiutano a soddisfare gli obiettivi di sicurezza. Questi strumenti rispecchiano i familiari controlli distribuiti negli ambienti On-Premise. AWS fornisce caratteristiche e strumenti specifici per la sicurezza da usare per la gestione della configurazione, il controllo degli accessi e la sicurezza di rete e dei dati. AWS mette inoltre a disposizione strumenti di monitoraggio e registrazione che forniscono visibilità completa su ciò che accade nell'ambiente.

Argomenti

Sicurezza dell'infrastruttura

AWS offre diversi servizi e funzionalità per la sicurezza che aumentano la privacy e migliorano il controllo degli accessi di rete. Tra le soluzioni sono incluse le seguenti:

- Firewall di rete integrati in Amazon VPC che permettono di creare reti private e controllare l'accesso alle istanze o alle applicazioni. I clienti possono controllare la crittografia in transito con TLS nei servizi AWS.
- Opzioni di connettività che permettono di creare connessioni private o dedicate dall'ufficio o dall'ambiente On-Premise.
- Tecnologie di mitigazione degli attacchi DDoS che si applicano al livello 3 o 4, nonché al livello 7. È possibile applicare tali tecnologie come parte delle strategie di distribuzione di applicazioni e contenuti.
- Crittografia automatica di tutto il traffico nelle reti AWS globali e regionali tra strutture AWS protette.

Gestione dell'inventario e della configurazione

AWS offre un'ampia gamma di strumenti che permettono di operare rapidamente mantenendo nel contempo la conformità delle risorse cloud agli standard e alle best practice dell'organizzazione. Tra le soluzioni sono incluse le seguenti:

- Strumenti di distribuzione per gestire la creazione e la disattivazione delle risorse AWS in base agli standard dell'organizzazione.
- Strumenti di gestione dell'inventario e della configurazione per identificare le risorse AWS nonché monitorare e gestire le modifiche a tali risorse nel tempo.
- Strumenti di definizione e gestione dei modelli per creare macchine virtuali standard, preconfigurate e con protezione avanzata per le istanze EC2.

Crittografia dei dati

AWS offre la possibilità di aggiungere un livello di sicurezza ai dati inattivi nel cloud grazie a caratteristiche di crittografia scalabili ed efficaci. Tra le soluzioni sono incluse le seguenti:

- Caratteristiche di crittografia dei dati a riposo disponibili nella maggior parte dei servizi AWS, come Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda e Amazon SageMaker.
- Opzioni flessibili di gestione delle chiavi, tra cui AWS Key Management Service, che consentono di scegliere se demandare la gestione delle chiavi di crittografia ad AWS oppure se mantenervi un controllo manuale completo.
- Archiviazione delle chiavi di crittografia basata su hardware e dedicata tramite AWS CloudHSM, per soddisfare i requisiti di conformità.
- Code dei messaggi crittografate per la trasmissione dei dati sensibili tramite la crittografia lato server (SSE, Server-Side Encryption) per Amazon SQS.

AWS fornisce inoltre API che permettono di integrare la crittografia e la protezione dei dati in qualsiasi servizio sviluppato o distribuito in un ambiente AWS.

Controllo di accessi e identità

AWS offre funzionalità per definire, applicare e gestire le policy di accesso utente nei servizi AWS. Tra le soluzioni sono incluse le seguenti:

- AWS Identity and Access Management (IAM) permette di definire singoli account utente con autorizzazioni per le risorse AWS, mentre AWS Multi-Factor Authentication permette di gestire account con privilegi con opzioni per autenticatori basati su software e hardware. È possibile usare IAM per concedere a dipendenti e applicazioni accesso federato alla AWS Management Console e alle API del servizio AWS usando i sistemi di gestione delle identità esistenti, come Microsoft Active Directory o altre offerte dei partner.
- AWS Directory Service permette l'integrazione e la federazione con le directory aziendali per ridurre il lavoro amministrativo e migliorare l'esperienza utente.
- AWS Single Sign-On (AWS SSO) permette di gestire le autorizzazioni utente e l'accesso SSO per tutti gli account da un'unica posizione centrale in AWS Organizations.

AWS offre integrazione nativa di Identity and Access Management in numerosi servizi, nonché integrazione delle API con qualsiasi applicazione o servizio.

Monitoraggio e registrazione

AWS fornisce strumenti e caratteristiche per ottenere informazioni su ciò che accade nell'ambiente AWS. Tra le soluzioni sono incluse le seguenti:

- Con AWS CloudTrail, puoi monitorare le implementazioni AWS nel cloud ottenendo lo storico delle chiamate API AWS del tuo account, comprese quelle effettuate tramite AWS Management Console, gli SDK AWS, gli strumenti a riga di comando e i servizi AWS di livello superiore. È anche possibile identificare quali utenti e account hanno chiamato le API AWS per i servizi che supportano CloudTrail, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute.
- Amazon CloudWatch fornisce una soluzione di monitoraggio affidabile, scalabile e flessibile pronta all'uso in pochi minuti. Non sarà più necessario configurare, gestire e dimensionare i sistemi di monitoraggio e l'infrastruttura.
- Amazon GuardDuty è un servizio di rilevamento delle minacce che esegue un monitoraggio continuo per individuare attività dannose e comportamenti non autorizzati al fine di proteggere carichi di lavoro e account AWS. Amazon GuardDuty espone le notifiche tramite Amazon CloudWatch in modo che sia possibile attivare una risposta automatica o inviare una notifica a un utente.

Questi strumenti e caratteristiche offrono la visibilità necessaria per individuare i problemi prima che abbiano ripercussioni sull'azienda, migliorare l'assetto di sicurezza e ridurre il profilo di rischio dell'ambiente in uso.

Prodotti per la sicurezza in Marketplace AWS

Il trasferimento dei carichi di lavoro di produzione in AWS può consentire alle organizzazioni di migliorare l'agilità, la scalabilità, l'innovazione e i risparmi sui costi, pur mantenendo un ambiente sicuro. Marketplace AWS offre prodotti leader nel settore della sicurezza equivalenti, identici o integrati con i controlli esistenti negli ambienti On-Premise. Questi prodotti integrano i servizi AWS esistenti per permettere di implementare un'architettura di sicurezza completa e un'esperienza più fluida nel cloud e negli ambienti On-Premise.

Indicazioni sulla sicurezza

AWS offre ai clienti indicazioni ed esperienza tramite supporto, risorse e strumenti online, nonché servizi professionali a cura di AWS e dei suoi partner.

AWS Trusted Advisor è uno strumento online che funge da esperto cloud personalizzato e aiuta a configurare le risorse nel rispetto delle best practice. Trusted Advisor analizza l'ambiente AWS per aiutare a colmare le lacune nella sicurezza e a individuare opportunità di risparmiare denaro, migliorare le prestazioni dei sistemi e aumentare l'affidabilità.

I team degli account AWS forniscono il primo punto di contatto per guidare l'utente nella distribuzione e nell'implementazione, indicando le risorse più adatte per risolvere eventuali problemi di sicurezza riscontrati.

Il supporto AWS Enterprise assicura tempi di risposta di 15 minuti e disponibilità 24 ore su 24, 7 giorni su 7, tramite telefono, chat o e-mail, oltre che un Technical Account Manager dedicato. Grazie a questo servizio, i problemi dei clienti vengono gestiti nel modo più rapido possibile.

La Rete dei partner AWSoffre centinaia di prodotti leader del settore equivalenti o identici ai controlli esistenti negli ambienti On-Premise o che si integrano con tali controlli. Questi prodotti integrano i servizi AWS esistenti per permettere di implementare un'architettura di sicurezza completa e un'esperienza più fluida nel cloud e negli ambienti On-Premise. Sono inoltre disponibili in tutto il mondo centinaia di partner di consulenza AWS certificati che forniscono supporto in merito alle esigenze di sicurezza e conformità.

La best practice relativa a sicurezza, rischi e conformità dei Servizi professionali AWS aiuta i clienti ad acquisire familiarità e sviluppare competenze tecniche quando viene eseguita la migrazione dei carichi di lavoro più sensibili in AWS Cloud. I Servizi professionali AWS supportano i clienti nello sviluppo di policy e best practice basate su modelli ben collaudati, per assicurare che l'assetto di sicurezza dei clienti soddisfi i requisiti di conformità interni ed esterni.

Marketplace AWS è un catalogo digitale con migliaia di offerte di software proposte da fornitori di software indipendenti che semplificano l'individuazione, il test, l'acquisto e l'implementazione del software in esecuzione su AWS. Marketplace AWS I prodotti di sicurezza integrano i servizi AWS esistenti per permettere di implementare un'architettura di sicurezza completa e un'esperienza più fluida nel cloud e negli ambienti On-Premise.

I bollettini sulla sicurezza di AWS forniscono informazioni sulle vulnerabilità e sulle minacce correnti, permettendo ai clienti di collaborare con gli esperti di sicurezza AWS per affrontare problemi come

la segnalazione di casi di uso illecito, le vulnerabilità e i test di penetrazione (pen-test). Sono inoltre disponibili risorse online per la segnalazione di vulnerabilità.

La documentazione sulla sicurezza di AWSillustra come configurare i servizi AWS per soddisfare gli obiettivi di sicurezza e conformità. I clienti AWS possono trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

AWS Well-Architected Framework aiuta chi progetta le architetture cloud a creare un'infrastruttura sicura, ad alte prestazioni, resiliente ed efficiente per le applicazioni. Il Canone di architettura AWS include un pilastro della sicurezza finalizzato alla protezione di informazioni e sistemi. Gli argomenti chiave includono la riservatezza e l'integrità dei dati, l'identificazione e la gestione dei privilegi per i diversi utenti, la protezione dei sistemi e la messa a punto di controlli per rilevare eventi legati alla sicurezza. I clienti possono utilizzare AWS Well-Architected Tool di AWS Management Console o avvalersi dei servizi di uno dei partner APN per assisterli.

AWS Well-Architected Tool aiuta ad analizzare lo stato dei carichi di lavoro e confrontarli rispetto alle più recenti best practice nell'ambito dell'architettura di AWS. Questo strumento gratuito è disponibile nella AWS Management Console e richiede di rispondere a una serie di domande relative a eccellenza operativa, sicurezza, affidabilità, efficienza delle prestazioni e ottimizzazione dei costi. AWS Well-Architected Tool fornisce quindi un piano per la progettazione del cloud in base a best practice definite.

Conformità

Le caratteristiche AWS per la conformità aiutano i clienti a comprendere i robusti controlli applicati da AWS per mantenere la sicurezza e la protezione dei dati in AWS Cloud. Quando vengono creati sistemi in AWS Cloud, AWS e i clienti condividono le responsabilità di conformità. Gli ambienti informatici AWS sono sottoposti a verifiche continue, con certificazioni rilasciate da enti di accreditamento in aree geografiche e mercati verticali, tra cui SOC 1/SSAE 16/ISAE 3402 (precedentemente SAS 70), SOC 2, SOC 3, ISO 9001/ISO 27001, FedRAMP, DoD SRG e PCI DSS Livello 1.i. Inoltre, AWS ha predisposto programmi di garanzia che forniscono modelli e mappature di controllo per aiutare i clienti a stabilire la conformità dei loro ambienti in esecuzione su AWS. Per un elenco completo dei programmi, consulta Programmi per la conformità in AWS.

Possiamo confermare che tutti i servizi AWS possono essere usati in conformità con il GDPR. Ciò significa che oltre a usufruire dei vantaggi derivanti da tutte le misure già adottate da AWS per mantenere la sicurezza dei servizi, i clienti possono distribuire i servizi AWS nell'ambito dei piani di conformità al GDPR. AWS offre un Addendum sul trattamento dei dati conforme al GDPR (GDPR DPA) che consente di soddisfare gli obblighi contrattuali stabiliti dal GDPR. Il documento AWS GDPR DPA è incorporato nei termini del servizio AWS e si applica automaticamente a tutti i clienti a livello globale che ne necessitano per la conformità al GDPR. Amazon.com, Inc. è un'azienda certificata ai sensi dello scudo UE-USA per la privacy e questa certificazione copre anche AWS. In questo modo, i clienti che scelgono di trasferire i dati personali negli Stati Uniti possono soddisfare gli obblighi in materia di protezione dei dati. La certificazione di Amazon.com Inc. è disponibile nel sito Web dello scudo UE-USA per la privacy: https://www.privacyshield.gov/list

Operando in un ambiente accreditato, i clienti riducono l'ambito e il costo delle revisioni da eseguire. L'infrastruttura sottostante di AWS viene continuamente sottoposta a valutazioni, che comprendono la sicurezza fisica e ambientale dell'hardware e dei data center, pertanto i clienti possono sfruttare i vantaggi di tali certificazioni e dei controlli correlati.

In un data center tradizionale le attività comuni relative alla conformità vengono spesso eseguite in modo manuale e a cadenza periodica. Tali attività includono la verifica delle configurazioni degli asset e la creazione di report relativi alle attività amministrative. I report risultanti, inoltre, diventano obsoleti ancora prima di venire pubblicati. Operando in un ambiente AWS i clienti possono usufruire dei vantaggi di strumenti automatici incorporati comeAWS Security Hub,AWS Config e AWS CloudTrail per la convalida della conformità. Questi strumenti riducono il lavoro necessario per le verifiche in quanto le attività diventano di routine, continuative e automatizzate. Dovendo dedicare meno

tempo alle attività manuali, chi si occupa della conformità in azienda non è più oberato dal carico amministrativo e può quindi occuparsi di gestire i rischi e migliorare l'assetto di sicurezza.

Approfondimenti

Per ulteriori informazioni, consulta le seguenti risorse:

Per informazioni su…	Consulta
Argomenti chiave, aree di ricerca e opportunità di formazione per la sicurezza cloud in AWS	Formazione sulla sicurezza in AWS Cloud
AWS Cloud Adoption Framework, che fornisce indicazioni organizzate in sei aree di interesse : azienda, persone, governance, piattaforma, sicurezza e operazioni	AWS Cloud Adoption Framework
Controlli specifici applicati in AW, come integrare AWS nel framework esistente	Amazon Web Services: rischio e conformità
Best practice per la sicurezza, l'identità e la conformità	Best practice per la sicurezza, l'identità e la conformità
Principio della sicurezza - AWS Well-Arch itected Framework	Principio della sicurezza - AWS Well-Arch itected Framework

Revisioni del documento

Per ricevere una notifica sugli aggiornamenti di questo whitepaper, iscriviti al feed RSS.

update-history-change	update-history-description	update-history-date
Whitepaper aggiornato	Aggiornato con i link per gli approfondimenti.	11 novembre 2021
Whitepaper aggiornato	Aggiornamento con i servizi, le risorse e le tecnologie più recenti.	22 gennaio 2020
Pubblicazione iniziale	Pubblicata l'introduzione alla sicurezza di AWS.	1 luglio 2015

Avvisi

I clienti sono responsabili della propria 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 soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e dei 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 e gli obblighi di AWS verso i propri clienti sono disciplinati dagli accordi AWS e il presente documento non fa parte né modifica alcun accordo tra AWS e i suoi clienti.