Pilastro della sicurezza

Canone di architettura AWS

Luglio 2020

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.

Sommario

Riassunto

Questo documento è incentrato sul pilastro della sicurezza del Canone di architettura. Fornisce linee guida per aiutarti ad applicare le best practice e le raccomandazioni correnti nella progettazione, distribuzione e manutenzione di carichi di lavoro sicuri in AWS.

Introduzione

Il Canone di architettura AWS aiuta a comprendere i pro e i contro delle decisioni che vengono prese durante la creazione di carichi di lavoro in AWS. Utilizzando il Canone, scoprirai le attuali best practice architetturali per progettare e gestire carichi di lavoro affidabili, sicuri, efficienti e convenienti nel cloud. Permette di misurare in modo coerente il carico di lavoro rispetto alle best practice e di identificare le aree da migliorare. Disporre di carichi di lavoro well-architected aumenta notevolmente la probabilità di successo aziendale.

Il Canone si basa su cinque principi:

- Eccellenza operativa
- Sicurezza
- Affidabilità
- Efficienza delle prestazioni
- Ottimizzazione dei costi

Questo documento è incentrato sul pilastro della sicurezza. Ti aiuterà a soddisfare i requisiti aziendali e normativi seguendo le attuali raccomandazioni di AWS. È rivolto a coloro che ricoprono ruoli tecnologici, ad esempio direttori tecnici, responsabili della sicurezza delle informazioni, architetti, sviluppatori e membri dei team operativi.

Grazie a questo documento, comprenderai le attuali raccomandazioni e strategie di AWS da utilizzare durante la progettazione di architetture cloud tenendo incentrandole sulla sicurezza. Questo documento non fornisce dettagli sull'implementazione o modelli architetturali; tuttavia, include riferimenti alle risorse appropriate in cui trovare tali informazioni. Adottando le prassi di questo documento, puoi creare architetture in grado di proteggere dati e sistemi, che controllino gli accessi e rispondano automaticamente agli eventi di sicurezza.

Sicurezza

Il pilastro della sicurezza descrive come sfruttare le tecnologie cloud per proteggere dati, sistemi e asset in modo da migliorare l'assetto di sicurezza. Questo documento fornisce linee guida dettagliate sulle best practice per la progettazione di carichi di lavoro sicuri in AWS.

Principi di progettazione

Nel cloud sono presenti diversi principi utili per rafforzare la sicurezza del carico di lavoro:

- **Implementazione di una solida base di identità:** implementa il principio del privilegio minimo e applica la separazione dei compiti assegnando l'autorizzazione appropriata per ogni interazione con le risorse AWS. Centralizza la gestione delle identità e mira a eliminare la dipendenza dalle credenziali statiche a lungo termine.
- **Abilitazione della tracciabilità:** monitora, crea avvisi e verifica in tempo reale le operazioni e le modifiche apportate al tuo ambiente. Integra la raccolta di log e parametri con i sistemi per analizzare e intervenire automaticamente.
- **Applicazione della sicurezza a tutti i livelli:** applica un approccio di difesa avanzata con più controlli di sicurezza. Applicalo a tutti i livelli (ad esempio, edge di rete, VPC, bilanciamento del carico, ogni istanza e servizio di elaborazione, sistema operativo, applicazione e codice).
- **Automatizzazione delle best practice di sicurezza:** i meccanismi di sicurezza automatizzati basati su software migliorano la capacità di ricalibrare le risorse in modo sicuro, più rapido e conveniente. Crea architetture sicure, compresa l'implementazione dei controlli, che sono definite e gestite come codice nei modelli controllati dalle versioni.
- **Protezione dei dati in transito e inattivi**: classifica i dati in base a livelli di sensibilità e utilizza meccanismi quali crittografia, tokenizzazione e controllo degli accessi, ove opportuno.
- **Accesso limitato delle persone ai dati**: utilizza meccanismi e strumenti per ridurre o eliminare l'esigenza di accesso diretto o di elaborazione manuale dei dati. Ciò riduce il rischio di perdita, modifica e altri errori umani durante la gestione dei dati sensibili.
- **Preparazione agli eventi di sicurezza:** preparati per un incidente creando policy e processi di analisi e gestione degli incidenti allineati ai requisiti dell'organizzazione. Esegui simulazioni di risposta agli incidenti e utilizza strumenti dotati di automazione per aumentare la velocità nel rilevamento, nell'indagine e nel ripristino.

Definizione

La sicurezza nel cloud comprende cinque aree:

1. Identity and Access Management
2. Rilevamento
3. Protezione dell'infrastruttura
4. Protezione dei dati
5. Risposta agli incidenti

La sicurezza e la conformità sono responsabilità condivise tra AWS e il cliente. Questo modello condiviso può contribuire a ridurre il carico operativo. I clienti devono valutare con attenzione i servizi scelti, dato che le loro responsabilità variano in base ai servizi utilizzati, all'integrazione di tali servizi nel loro ambiente IT e alle leggi e ai regolamenti applicabili. La natura di questa responsabilità condivisa fornisce inoltre la flessibilità e il controllo che consentono la distribuzione.

Gestione sicura del carico di lavoro

Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati con le raccomandazioni di AWS e del settore nonché con l'intelligence sulle minacce aiuta a sviluppare il modello di rischio e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida consentono di ricalibrare le operazioni di sicurezza.

Identificazione dei rischi e classificazione in ordine di priorità utilizzando un modello di rischio: utilizza un modello di rischio per identificare e mantenere un registro aggiornato delle potenziali minacce. Classifica le minacce in ordine di priorità e adatta i controlli di sicurezza in modo da prevenirle, rilevarle e affrontarle. Rivedi e mantieni questo approccio nel contesto dell'evoluzione del panorama della sicurezza.

Identificazione e convalida degli obiettivi di controllo: in base ai requisiti di conformità e ai rischi identificati dal modello di rischio, ottieni e convalida gli obiettivi di controllo e i controlli da applicare al carico di lavoro. La convalida continua degli obiettivi di controllo e dei controlli aiuta a misurare l'efficacia della mitigazione dei rischi.

Aggiornamento costante sulle minacce alla sicurezza: riconosci i vettori di attacco rimanendo aggiornato sulle le minacce alla sicurezza più recenti per definire e implementare controlli appropriati.

Aggiornamento costante sulle raccomandazioni circa la sicurezza: resta aggiornato sulle raccomandazioni da parte di AWS e del settore in merito alla sicurezza, così da sviluppare l'assetto di sicurezza del carico di lavoro.

Valutazione e implementazione regolare di nuovi servizi e funzionalità di sicurezza: valuta e implementa servizi e funzionalità di sicurezza di AWS e partner APN che consentano di sviluppare l'assetto di sicurezza del carico di lavoro.

Automatizzazione dei test e convalida dei controlli di sicurezza nelle pipeline: stabilisci previsioni e modelli sicuri per i meccanismi di sicurezza testati e convalidati come parte della compilazione, delle pipeline e dei processi. Utilizza strumenti e l'automazione per testare e convalidare tutti i controlli di sicurezza in modo continuo. Ad esempio, scansiona elementi quali immagini di macchine e modelli di infrastrutture come codice per individuare vulnerabilità di sicurezza, irregolarità e deviazioni da una previsione stabilita in ogni fase.

È fondamentale ridurre il numero di errori di sicurezza introdotti in un ambiente di produzione, quindi più operazioni di controllo di qualità e riduzione dei difetti è possibile eseguire nel processo di compilazione, più efficace sarà il risultato. Progetta pipeline di integrazione e distribuzione continue (CI/CD) per testare eventuali problemi di sicurezza quando possibile. Le pipeline CI/CD offrono l'opportunità di migliorare la sicurezza in ogni fase della compilazione e della distribuzione. Anche gli strumenti di sicurezza CI/CD devono essere mantenuti aggiornati per mitigare le minacce in continua evoluzione.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni su come gestire il carico di lavoro in modo sicuro.

Video

- Security Best Practices the Well-Architected Way
- Enable AWS adoption at scale with automation and governance
- AWS Security Hub: Manage Security Alerts & Automate Compliance
- Automate your security on AWS

Documentazione

- Panoramica dei processi di sicurezza
- Bollettini sulla sicurezza
- Blog sulla sicurezza
- Novità di AWS
- AWS Security Audit Guidelines
- Set Up a CI/CD Pipeline on AWS

Gestione e separazione degli account AWS

Ti consigliamo di organizzare i carichi di lavoro in account e account di gruppo separati in base alla funzione, ai requisiti di conformità o a un set comune di controlli anziché riflettere la struttura della reportistica dell'organizzazione. In AWS, gli account sono un container dai confini difficoltosi e inaffidabile per le risorse. Ad esempio, la separazione a livello di account è fortemente consigliata per isolare i carichi di lavoro di produzione dai carichi di lavoro di sviluppo e test.

Carichi di lavoro separati utilizzando gli account: inizia tenendo conto della sicurezza e dell'infrastruttura per consentire alla tua organizzazione di impostare limiti comuni man mano che i carichi di lavoro aumentano. Questo approccio fornisce limiti e controlli tra i carichi di lavoro. La separazione a livello di account è fortemente consigliata per isolare gli ambienti di produzione dagli ambienti di sviluppo e test, oppure per fornire un forte limite logico tra i carichi di lavoro che elaborano dati con diversi livelli di sensibilità, secondo quanto definito da requisiti di conformità esterni (ad esempio PCI-DSS o HIPAA), e i carichi di lavoro che non lo fanno.

Protezione degli account AWS: la protezione degli account AWS prevede diversi aspetti, tra cui la protezione di e il non utilizzo dell'utente root e l'aggiornamento costante delle informazioni di contatto. Puoi utilizzare AWS Organizations per gestire e amministrare centralmente i tuoi account man mano che i tuoi carichi di lavoro crescono e li ridimensioni. AWS Organizations ti aiuta a gestire gli account, impostare controlli e configurare i servizi tra gli account.

Gestione centralizzata degli account: AWS Organizations automatizza la creazione e la gestione di account AWS e il controllo di tali account dopo la loro creazione. Quando crei un account tramite AWS Organizations, è importante considerare l'indirizzo e-mail utilizzato, in quanto questo sarà l'utente root che consente la reimpostazione della password. Organizations consente di raggruppare gli account in unità organizzative (UO), che possono rappresentare ambienti diversi in base ai requisiti e allo scopo del carico di lavoro.

Impostazione dei controlli a livello centrale: controlla le operazioni che gli account AWS possono eseguire consentendo solo servizi, regioni e azioni del servizio specifici al livello appropriato. AWS Organizations consente di utilizzare le policy di controllo dei servizi (SCP) per applicare limiti alle autorizzazioni a livello di organizzazione, unità organizzativa o account, validi per tutti gli utenti e ruoli AWS Identity and Access Management (IAM). Ad esempio, è possibile applicare una SCP che limita agli utenti l'avvio di risorse in regioni che non sono state esplicitamente consentite. AWS Control Tower offre un modo semplificato per configurare e gestire più account. Automatizza la configurazione degli account in AWS Organizations, automatizza il provisioning, applica limiti (che includono prevenzione e rilevamento) e fornisce un pannello di controllo per la visibilità.

Configurazione di servizi e risorse centralmente: AWS Organizations ti aiuta a configurare i servizi AWS applicabili a tutti i tuoi account. Ad esempio, puoi configurare la registrazione centralizzata di tutte le operazioni eseguite nell'organizzazione utilizzando AWS CloudTrail e impedire agli account membri di disabilitare la registrazione. Puoi inoltre aggregare

centralmente i dati per le regole definite utilizzando AWS Config, in modo da controllare i tuoi carichi di lavoro per verificare la conformità e reagire rapidamente alle modifiche. AWS CloudFormation StackSets consente di gestire in modo centralizzato gli stack di AWS CloudFormation negli account e nelle unità organizzative della tua organizzazione. In questo modo puoi effettuare automaticamente il provisioning di un nuovo account per soddisfare i requisiti di sicurezza.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle raccomandazioni AWS relative alla distribuzione e alla gestione di più account AWS.

Video

- Managing and governing multi-account AWS environments using AWS Organizations
- AXA: Scaling adoption with a Global Landing Zone
- Using AWS Control Tower to Govern Multi-Account AWS Environments

Documentazione

- Establishing your best practice AWS environment
- AWS Organizations
- AWS Control Tower
- Utilizzo del AWS CloudFormation StackSets
- How to use service control policies to set permission guardrails across accounts in your AWS Organization

Laboratori pratici

- Laboratorio: AWS Account and Root User

Identity and Access Management

Per utilizzare i servizi AWS, devi concedere agli utenti e alle applicazioni l'accesso alle risorse nei tuoi account AWS. Quando esegui più carichi di lavoro su AWS, hai bisogno di una solida gestione delle identità e autorizzazioni per garantire che le persone giuste abbiano accesso alle risorse corrette in condizioni appropriate. AWS offre un'ampia gamma di funzionalità per aiutarti a gestire le identità di persone e macchine e le relative autorizzazioni. Le best practice per queste funzionalità rientrano in due aree principali:

- Gestione delle identità
- Gestione delle autorizzazioni

Gestione delle identità

Esistono due tipi di identità che è necessario gestire quando si utilizzano carichi di lavoro AWS sicuri.

Identità umane: gli amministratori, gli sviluppatori, gli operatori e i fruitori di applicazioni necessitano di un'identità per accedere agli ambienti e alle applicazioni AWS. Possono essere membri dell'organizzazione o utenti esterni con cui collabori e che interagiscono con le tue risorse AWS tramite browser Web, applicazioni client, app mobili o strumenti a riga di comando interattivi.

Identità di macchine: le applicazioni per il carico di lavoro, gli strumenti operativi e i componenti necessitano di un'identità per effettuare richieste ai servizi AWS, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nell'ambiente AWS, ad esempio istanze Amazon EC2 o funzioni AWS Lambda. Puoi anche gestire le identità di macchine per soggetti esterni che necessitano dell'accesso. Inoltre, potresti disporre di macchine al di fuori di AWS che devono accedere al tuo ambiente AWS.

Fai affidamento su un provider di identità centralizzato

Per le identità della forza lavoro, affidati a un provider di identità che ti consenta di gestire le identità in un luogo centralizzato. In questo modo è più semplice gestire l'accesso tra più applicazioni e servizi, perché crei, gestisci e revochi l'accesso da una singola posizione. Ad esempio, se qualcuno lascia la tua organizzazione, puoi revocare l'accesso per tutte le applicazioni e i servizi (incluso AWS) da un'unica posizione. Ciò riduce la necessità di molteplici credenziali e offre l'opportunità di integrarsi con i processi delle risorse umane esistenti.

Per la federazione con singoli account AWS, puoi utilizzare identità centralizzate per AWS con un provider basato su SAML 2.0 con AWS IAM. Puoi utilizzare qualsiasi provider in hosting su AWS, esterno ad AWS o fornito da AWS Partner Network (APN), compatibile con il protocollo SAML 2.0. Puoi utilizzare la federazione tra l'account AWS e il provider scelto

per concedere a un utente o a un'applicazione l'accesso per chiamare le operazioni API AWS utilizzando un'asserzione SAML per ottenere le credenziali di sicurezza temporanee. È inoltre supportato il Single Sign-On basato sul Web, che consente agli utenti di accedere alla Console di gestione AWS dal portale di accesso.

Per la federazione a più account in AWS Organizations, puoi configurare l'origine di identità in AWS Single Sign-On (AWS SSO) e specificare dove sono archiviati gli utenti e i gruppi. Una volta configurato, il provider di identità è la tua fonte di attendibilità e puoi sincronizzare le informazioni utilizzando il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Puoi quindi cercare utenti o gruppi e concedere loro l'accesso Single Sign-On ad account AWS, applicazioni cloud o entrambi.

AWS SSO si integra con AWS Organizations consentendoti di configurare il provider di identità una volta e quindi concedere l'accesso agli account nuovi e esistenti gestiti nella tua organizzazione. AWS SSO fornisce uno store predefinito che puoi utilizzare per gestire utenti e gruppi. Se scegli di utilizzare lo store AWS SSO, crea utenti e gruppi e assegna il loro livello di accesso agli account e alle applicazioni AWS, tenendo presente la best practice del privilegio minimo. In alternativa, puoi scegliere di connetterti al provider di identità esterno utilizzando SAML 2.0 o connetterti a Microsoft AD Directory utilizzando AWS Directory Service. Una volta configurate, puoi accedere alla Console di gestione AWS, all'interfaccia a riga di comando o all'app mobile AWS, eseguendo l'autenticazione tramite il tuo provider di identità centrale.

Per gestire gli utenti finali o i consumatori dei tuoi carichi di lavoro, ad esempio un'app per dispositivi mobili, puoi utilizzare Amazon Cognito. Ti consente di autenticare, autorizzare e gestire utenti per applicazioni Web e per dispositivi mobili. Gli utenti possono accedere direttamente con un nome utente e una password oppure tramite terze parti, ad esempio Amazon, Apple, Facebook o Google.

Sfrutta i gruppi di utenti e gli attributi

Man mano che il numero di utenti gestiti cresce, sarà necessario determinare i modi per organizzarli in modo da poterli gestire su vasta scala. Inserisci gli utenti con requisiti di sicurezza comuni in gruppi definiti dal provider di identità e metti in atto meccanismi per garantire che gli attributi utente che potrebbero essere utilizzati per il controllo degli accessi (ad esempio, reparto o posizione) siano corretti e aggiornati. Utilizza questi gruppi e attributi, anziché i singoli utenti, per controllare l'accesso. In questo modo puoi gestire l'accesso centralmente, modificando una volta sola l'appartenenza o gli attributi di un gruppo utente con un set di autorizzazioni, anziché aggiornare numerose policy individuali quando le esigenze di accesso di un utente cambiano. Puoi utilizzare AWS SSO per gestire gruppi di utenti e attributi. AWS SSO supporta la maggior parte degli attributi utilizzati, indipendentemente dal fatto che vengano inseriti manualmente durante la creazione dell'utente o assegnati automaticamente utilizzando un motore di sincronizzazione, come definito nella specifica System for Cross-Domain Identity Management (SCIM).

Utilizza meccanismi di accesso efficaci

Imposta la lunghezza minima della password e spiega agli utenti la necessità di evitare password comuni o utilizzate in precedenza. Applica la Multi-Factor Authentication (MFA) con meccanismi software o hardware per garantire un ulteriore livello di verifica. Ad esempio, quando utilizzi AWS SSO come origine di identità, configura l'impostazione "Compatibile con il contesto" o "Sempre attivo" per MFA e consenti agli utenti di registrare i propri dispositivi MFA per accelerare l'adozione. Quando utilizzi un provider di identità (IdP) esterno, configura il provider di identità per MFA.

Utilizza credenziali temporanee

Richiedi alle identità di acquisire dinamicamente credenziali temporanee. Per le identità della forza lavoro, utilizza AWS SSO o la federazione con IAM per accedere agli account AWS. Per le identità di macchine, ad esempio le istanze EC2 o le funzioni Lambda, è necessario utilizzare ruoli IAM anziché utenti IAM con chiavi di accesso a lungo termine.

Per le identità umane che utilizzano la Console di gestione AWS, è necessario che gli utenti acquisiscano credenziali temporanee ed eseguano la federazione in AWS. A tale scopo, puoi utilizzare il portale utente AWS SSO o configurare la federazione con IAM. Per gli utenti che richiedono l'accesso all'interfaccia a riga di comando (CLI), assicurati di utilizzare AWS CLI v2, che supporta l'integrazione diretta con AWS Single Sign-On (AWS SSO). Gli utenti possono creare profili CLI collegati ad account e ruoli AWS SSO. Il CLI recupera automaticamente le credenziali AWS da AWS SSO e le aggiorna per tuo conto. In questo modo non è più necessario copiare e incollare credenziali AWS temporanee dalla console AWS SSO. Per l'SDK, gli utenti devono fare affidamento su AWS STS per acquisire ruoli per ricevere credenziali temporanee. In alcuni casi, le credenziali temporanee potrebbero non essere pratiche. È necessario conoscere i rischi che comporta l'archiviazione delle chiavi di accesso, ruotarle spesso e richiedere l'autenticazione MFA come condizione quando possibile.

Per i casi in cui è necessario concedere ai consumatori l'accesso alle risorse AWS, utilizza i pool di identità di Amazon Cognito e assegna loro un set di credenziali temporanee con privilegi limitati per accedere alle risorse AWS. Le autorizzazioni per ogni utente sono controllate tramite i ruoli IAM creati. Puoi definire regole per scegliere il ruolo per ogni utente in base alle registrazioni nel token ID dell'utente. Puoi definire un ruolo predefinito per gli utenti autenticati. Puoi anche definire un ruolo IAM separato con autorizzazioni limitate per gli utenti guest non autenticati.

Per le identità di macchine, è necessario fare affidamento sui ruoli IAM per concedere l'accesso ad AWS. Per le istanze EC2, puoi utilizzare i ruoli per Amazon EC2. Puoi collegare un ruolo IAM all'istanza EC2 per consentire alle applicazioni in esecuzione su Amazon EC2 di utilizzare credenziali di sicurezza temporanee create, distribuite e fatte ruotare automaticamente da AWS. Per accedere alle istanze EC2 tramite chiavi o password,

AWS Systems Manager è un modo più sicuro per accedere e gestire le istanze utilizzando un agente preinstallato senza il segreto archiviato. Inoltre, altri servizi AWS, ad esempio AWS Lambda, consentono di configurare un ruolo del servizio IAM per concedere le autorizzazioni al servizio per eseguire operazioni AWS utilizzando credenziali temporanee.

Verifica e ruota periodicamente le credenziali

La convalida periodica, preferibilmente tramite uno strumento automatizzato, è necessaria per verificare che vengano applicati i controlli corretti. Per le identità umane, è necessario richiedere agli utenti di modificare periodicamente le password e ritirare le chiavi di accesso a favore delle credenziali temporanee. Ti consigliamo inoltre di monitorare in modo continuo le impostazioni MFA nel tuo provider di identità. Puoi configurare AWS Config Rules per monitorare queste impostazioni. Per le identità di macchine, devi fare affidamento sulle credenziali temporanee utilizzando i ruoli IAM. Per situazioni in cui ciò non è possibile, è necessario eseguire audit frequenti e ruotare le chiavi di accesso.

Archivia e utilizza i segreti in modo sicuro

Per le credenziali non correlate a IAM, ad esempio gli accessi al database, utilizza un servizio progettato per gestire i segreti, ad esempio AWS Secrets Manager. AWS Secrets Manager semplifica la gestione, la rotazione e lo storage sicuro delle chiavi segrete crittografate utilizzando i servizi supportati. Le chiamate per accedere ai segreti vengono registrate in CloudTrail ai fini dell'audit e le autorizzazioni IAM possono concedere loro un accesso con privilegi minimi.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle best practice di AWS per la protezione delle credenziali AWS.

Video

- Mastering identity at every layer of the cake
- Managing user permissions at scale with AWS SSO
- Best Practices for Managing, Retrieving, & Rotating Secrets at Scale

Documentazione

- L'utente root dell'account AWS
- Credenziali Utente root dell'account AWS rispetto a credenziali utente IAM
- Best practice per la sicurezza in IAM

- Impostazione di una policy sulle password dell'account per utenti IAM
- Nozioni di base su AWS Secrets Manager
- Utilizzo dei profili delle istanze
- Credenziali di sicurezza temporanee
- Provider di identità e federazione

Gestione delle autorizzazioni

Gestisci le autorizzazioni per controllare l'accesso alle identità di persone e macchine che richiedono l'accesso ad AWS e ai tuoi carichi di lavoro. Le autorizzazioni controllano chi può accedere a cosa e a quali condizioni. Imposta le autorizzazioni per specifiche identità umane e di macchine per concedere l'accesso a determinate azioni del servizio su risorse specifiche. Inoltre, specifica le condizioni che devono essere vere per concedere l'accesso. Ad esempio, puoi consentire agli sviluppatori di creare nuove funzioni Lambda, ma solo in una regione specifica. Quando gestisci gli ambienti AWS su vasta scala, attieniti alle seguenti best practice per garantire che le identità abbiano solo l'accesso necessario e nient'altro.

Definizione dei limiti per le autorizzazioni dell'organizzazione

Man mano che aumenti e gestisci carichi di lavoro aggiuntivi in AWS, devi separarli utilizzando gli account e gestire questi ultimi utilizzando AWS Organizations. Ti consigliamo di stabilire limiti di autorizzazione comuni che limitano l'accesso a tutte le identità nella tua organizzazione. Ad esempio, puoi limitare l'accesso a regioni AWS specifiche o impedire al tuo team di eliminare risorse comuni, come ad esempio un ruolo IAM utilizzato dal team di sicurezza centrale. Puoi iniziare implementando policy di controllo dei servizi di esempio, ad esempio impedendo agli utenti di disabilitare i servizi chiave.

Puoi utilizzare AWS Organizations per raggruppare gli account e impostare controlli comuni su ciascun gruppo di account. Per impostare questi controlli comuni, puoi utilizzare i servizi integrati con AWS Organizations. Nello specifico, puoi utilizzare le policy di controllo dei servizi (SCP) per limitare l'accesso al gruppo di account. Le policy di controllo dei servizi utilizzano il linguaggio di policy IAM e consentono di stabilire controlli a cui aderiscono tutti i principali IAM (utenti e ruoli). Puoi limitare l'accesso a specifiche azioni del servizio, risorse e in base a condizioni specifiche per soddisfare le esigenze di controllo degli accessi della tua organizzazione. Se necessario, puoi definire eccezioni ai limiti definiti. Ad esempio, puoi limitare le azioni del servizio per tutte le entità IAM nell'account tranne per un ruolo amministratore specifico.

Concessione dell'accesso con privilegi minimi

Stabilire un principio di privilegio minimo assicura che alle identità venga concesso di eseguire il minimo set di funzioni necessarie alla realizzazione di un'attività specifica, bilanciando al tempo stesso usabilità ed efficienza. Il funzionamento di questo principio limita l'accesso involontario e ti consente di verificare chi ha accesso a quali risorse. In AWS, le identità non dispongono di autorizzazioni per impostazione predefinita, ad eccezione dell'utente root, che deve essere utilizzato solo per alcune attività specifiche.

Puoi utilizzare le policy per concedere esplicitamente autorizzazioni collegate a IAM o entità di risorse, ad esempio un ruolo IAM utilizzato da identità federate o macchine o risorse (ad esempio, bucket S3). Quando crei e colleghi una policy, puoi specificare le azioni del servizio, le risorse e le condizioni che devono essere vere affinché AWS consenta l'accesso. AWS supporta un'ampia gamma di condizioni per aiutarti a ridurre l'accesso. Ad esempio, utilizzando la chiave di condizione `PrincipalOrgID`, l'identificatore di AWS Organizations viene verificato in modo che l'accesso possa essere concesso all'interno della tua organizzazione AWS. Puoi anche controllare le richieste effettuate dai servizi AWS per tuo conto, ad esempio AWS CloudFormation per la creazione di una funzione AWS Lambda, utilizzando la chiave di condizione `CalledVia`. In questo modo puoi impostare autorizzazioni granulari per le identità umane e di macchine in AWS.

AWS offre inoltre funzionalità che consentono di dimensionare la gestione delle autorizzazioni e rispettare i privilegi minimi.

Limiti delle autorizzazioni: puoi utilizzare i limiti delle autorizzazioni per impostare il numero massimo di autorizzazioni che un amministratore può impostare. In questo modo puoi delegare la possibilità di creare e gestire le autorizzazioni agli sviluppatori, ad esempio la creazione di un ruolo IAM, ma limitare le autorizzazioni che possono concedere in modo che non possano inoltrare il proprio privilegio utilizzando ciò che hanno creato.

Controllo degli accessi basato su attributi (ABAC): AWS consente di concedere autorizzazioni in base agli attributi. In AWS, questi sono denominati tag. I tag possono essere collegati ai principali IAM (utenti o ruoli) e alle risorse AWS. Utilizzando le policy IAM, gli amministratori possono creare una policy riutilizzabile che applica le autorizzazioni in base agli attributi dell'entità principale IAM. Ad esempio, in qualità di amministratore puoi utilizzare una singola policy IAM che concede agli sviluppatori dell'organizzazione l'accesso alle risorse AWS che corrispondono ai tag di progetto degli sviluppatori. Man mano che il team di sviluppatori aggiunge risorse ai progetti, le autorizzazioni vengono applicate automaticamente in base agli attributi. Di conseguenza, non è richiesto alcun aggiornamento delle policy per ogni nuova risorsa.

Analisi dell'accesso pubblico e tra account

In AWS, puoi concedere l'accesso alle risorse in un altro account. Puoi concedere l'accesso diretto tra account utilizzando policy collegate a risorse (ad esempio, policy di bucket S3) o consentendo a un'identità di assumere un ruolo IAM in un altro account. Nell'utilizzare le policy delle risorse, assicurati di concedere l'accesso alle identità nella tua organizzazione e di indicare quando rendi pubblica una risorsa. Poiché rendere pubblica una risorsa consente a chiunque di accedere alla risorsa, è necessario effettuare questa operazione con moderazione. IAM Access Analyzer utilizza metodi matematici (ovvero sicurezza comprovabile) per identificare tutti i percorsi di accesso a una risorsa dall'esterno del proprio account. Esamina continuamente le policy delle risorse e segnala i risultati dell'accesso pubblico e tra account per semplificare l'analisi di accessi potenzialmente estensivi.

Condivisione delle risorse in modo sicuro

Quando gestisci i carichi di lavoro utilizzando account separati, in alcuni casi sarà necessario condividere le risorse tra tali account. Ti consigliamo di condividere le risorse utilizzando AWS Resource Access Manager (AWS RAM). Questo servizio ti consente di condividere in modo semplice e sicuro le risorse AWS all'interno della tua organizzazione AWS e delle unità organizzative. Con AWS RAM l'accesso alle risorse condivise viene automaticamente concesso o revocato quando gli account vengono spostati da e verso l'organizzazione o l'unità organizzativa con cui sono condivisi. In questo modo puoi garantire che le risorse vengano condivise solo con gli account desiderati.

Riduzione delle autorizzazioni in modo continuo

A volte, quando i team e i progetti stanno per iniziare, puoi scegliere di concedere un accesso estensivo per promuovere innovazione e agilità. Ti consigliamo di valutare l'accesso in modo continuo e limitare l'accesso solo alle autorizzazioni richieste e ottenere il privilegio minimo. AWS fornisce funzionalità di analisi degli accessi per aiutarti a identificare gli accessi inutilizzati. Per aiutarti a identificare gli utenti e i ruoli inutilizzati, AWS analizza le attività di accesso e fornisce informazioni sull'ultimo ruolo e chiave di accesso utilizzati. Puoi utilizzare il timestamp dell'ultimo accesso per identificare utenti e ruoli inutilizzati e rimuoverli. Inoltre, puoi rivedere le informazioni sull'ultimo accesso al servizio e sull'ultima azione per identificare e restringere le autorizzazioni per specifici utenti e ruoli. Ad esempio, puoi utilizzare le informazioni sull'ultimo accesso per identificare le operazioni S3 specifiche richieste dal ruolo dell'applicazione e limitare l'accesso solo a quelle. Queste funzionalità sono disponibili nella console e a livello di programmazione per consentirti di incorporarle nei flussi di lavoro dell'infrastruttura e negli strumenti automatici.

Determinazione di un processo per l'accesso di emergenza

Devi disporre di un processo che consenta l'accesso di emergenza al carico di lavoro, in particolare i tuoi account AWS, nell'improbabile caso di un problema con un processo automatizzato o una pipeline. Questo processo potrebbe includere una combinazione di funzionalità diverse, ad esempio un ruolo AWS tra account di emergenza per l'accesso o un processo specifico che gli amministratori devono seguire per convalidare e approvare una richiesta di emergenza.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle attuali best practice di AWS per le autorizzazioni dettagliate.

Video

- Become an IAM Policy Master in 60 Minutes or Less
- Separation of Duties, Least Privilege, Delegation, & CI/CD

Documentazione

- Assegnare il privilegio minimo
- Lavorare con le policy
- Delegare le autorizzazioni per amministrare utenti, gruppi e credenziali IAM
- IAM Access Analyzer
- Rimuovere credenziali non necessarie
- Assumere un ruolo nel CLI con MFA
- Limiti delle autorizzazioni
- Controllo dell'accesso basato su attributi (Attribute-Based Access Control, ABAC)

Laboratori pratici

- Laboratorio: IAM Permission Boundaries Delegating Role Creation
- Laboratorio: IAM Tag Based Access Control for EC2
- Laboratorio: Lambda Cross Account IAM Role Assumption

Rilevamento

Il rilevamento consente di identificare un potenziale errore di configurazione della sicurezza, una minaccia o un comportamento imprevisto. È un aspetto fondamentale del ciclo di vita della sicurezza e può essere utilizzato per supportare un processo di qualità, un obbligo legale o di conformità, nonché per identificare e rispondere alle minacce. Esistono diversi tipi di meccanismi di rilevamento. Ad esempio, si possono analizzare i log del carico di lavoro per individuare gli exploit utilizzati. Devi esaminare regolarmente i meccanismi di rilevamento correlati al carico di lavoro per assicurarti di soddisfare le policy e i requisiti interni ed esterni. Gli avvisi e le notifiche automatizzati devono basarsi su condizioni definite per consentire ai team o agli strumenti di eseguire l'analisi. Questi meccanismi sono importanti fattori di reazione che possono aiutare l'organizzazione a identificare e comprendere l'ambito delle attività anomale.

In AWS, è possibile utilizzare diversi approcci per affrontare i meccanismi di rilevamento. Le seguenti sezioni descrivono come utilizzare questi approcci:

- Configurazione
- Analisi

Configurazione

Configurazione della registrazione di servizi e applicazioni: una pratica di base è quella di stabilire un set di meccanismi di rilevamento a livello di account. Questo set di meccanismi di base ha lo scopo di registrare e rilevare un'ampia gamma di operazioni su tutte le risorse nel tuo account. Tali meccanismi consentono di creare una funzionalità di rilevamento completa con opzioni che includono la correzione automatizzata e integrazioni dei partner per renderla ancora più funzionale.

In AWS, i servizi in questo set di base includono:

- AWS CloudTrail fornisce uno storico degli eventi delle attività del tuo account AWS, incluse le operazioni eseguite dalla Console di gestione AWS, gli SDK AWS, gli strumenti a riga di comando e altri servizi AWS.
- AWS Config monitora e registra le configurazioni delle risorse AWS e consente di automatizzare la valutazione e la correzione rispetto alle configurazioni desiderate.
- Amazon GuardDuty è un servizio di rilevamento delle minacce che esegue un monitoraggio costante per individuare attività dannose e comportamenti non autorizzati al fine di proteggere i tuoi carichi di lavoro e account AWS.
- AWS Security Hub offre un unico punto di aggregazione, organizzazione e assegnazione delle priorità degli agli avvisi di sicurezza o dei risultati provenienti da diversi servizi AWS e da prodotti opzionali di terze parti per fornirti una panoramica completa degli avvisi di sicurezza e dello stato di conformità.

Partendo dalla base esistente a livello di account, molti servizi AWS principali, ad esempio Amazon Virtual Private Cloud (VPC), forniscono funzionalità di registrazione a livello di servizio. I log di flusso VPC consentono di acquisire informazioni sul traffico IP da e verso le interfacce di rete che possono fornire approfondimenti preziosi sulla cronologia della connettività e attivare azioni automatizzate in base a comportamenti anomali.

Per le istanze EC2 e la registrazione basata su applicazioni che non provengono dai servizi AWS, i log possono essere archiviati e analizzati utilizzando Amazon CloudWatch Logs. Un agente raccoglie i log dal sistema operativo e dalle applicazioni in esecuzione e li archivia automaticamente. Quando i log sono disponibili in CloudWatch Logs, puoi elaborarli in tempo reale o analizzarli utilizzando Insights.

Oltre alla raccolta e all'aggregazione dei log, è altrettanto importante la capacità di estrarre informazioni significative dai grandi volumi di dati di log ed eventi generati da architetture complesse. Consulta la sezione sul *monitoraggio* del whitepaper Il pilastro dell'affidabilità per ulteriori dettagli. I log stessi possono contenere dati considerati sensibili, sia quando i dati dell'applicazione sono stati erroneamente inseriti nei file di log acquisiti dall'agente di CloudWatch Logs, sia quando la registrazione tra regioni è configurata per l'aggregazione dei log e vi sono considerazioni legislative sulla spedizione di determinati tipi di informazioni oltre confine.

Un approccio consiste nell'utilizzare le funzioni Lambda, attivate su eventi quando vengono distribuiti i log, per filtrare e redigere i dati di log prima di inoltrarli a una posizione di registrazione centrale, ad esempio un bucket S3. I log non redatti possono essere conservati in un bucket locale fino a quando non è trascorso un "periodo di tempo ragionevole" (secondo quanto stabilito dalla legislazione e dal team legale) e a quel punto una regola del ciclo di vita di S3 può eliminarli automaticamente. Si possono proteggere ulteriormente i log in Amazon S3 utilizzando S3 Object Lock, dove è possibile archiviare oggetti utilizzando un modello WORM (Write Once Read Many).

Analisi centralizzata di log, risultati e parametri: i team delle operazioni di sicurezza si affidano alla raccolta di log e all'utilizzo di strumenti di ricerca per individuare potenziali eventi di interesse, che potrebbero indicare attività non autorizzate o modifiche involontarie. Tuttavia, la semplice analisi dei dati raccolti e l'elaborazione manuale delle informazioni non sono sufficienti per tenere il passo con il volume di informazioni provenienti da architetture complesse. Le sole analisi e i soli resoconti non facilitano l'assegnazione delle risorse giuste per lavorare a un evento in modo adeguato e nei tempi giusti.

Una best practice per creare un team esperto per le operazioni di sicurezza consiste nell'integrare profondamente il flusso di eventi e risultati di sicurezza in un sistema di notifica e flusso di lavoro, ad esempio un sistema di ticketing, un sistema di bug o problemi o altri sistemi SIEM (Security Information and Event Management). Ciò elimina il flusso di lavoro da e-mail e report statici e consente di instradare, inoltrare e gestire eventi o risultati. Molte organizzazioni integrano anche gli avvisi di sicurezza nelle loro piattaforme di chat, collaborazione e di produttività per sviluppatori. Per le aziende che intraprendono la strada dell'automazione, un sistema di ticketing basato su API a bassa latenza offre una notevole flessibilità quando si pianifica "cosa automatizzare prima".

Questa best practice si applica non solo agli eventi di sicurezza generati dai messaggi di log che illustrano l'attività degli utenti o gli eventi di rete, ma anche a quelli generati dalle modifiche rilevate nell'infrastruttura stessa. La possibilità di rilevare le modifiche, determinare se una modifica è appropriata e quindi instradare tali informazioni al flusso di lavoro di correzione adatto è essenziale per mantenere e convalidare un'architettura sicura, in un contesto di modifiche difficili da individuare come indesiderabili per impedirne l'esecuzione tramite una combinazione di configurazioni IAM e Organizations.

GuardDuty e Security Hub forniscono meccanismi di aggregazione, deduplicazione e analisi per i record di log che vengono resi disponibili anche tramite altri servizi AWS. Nello specifico, GuardDuty acquisisce, aggrega e analizza le informazioni provenienti dal server DNS per il VPC e le informazioni altrimenti consultabili tramite CloudTrail e i log di flusso VPC. Security Hub è in grado di acquisire, aggregare e analizzare gli output di GuardDuty, AWS Config, Amazon Inspector, Macie, AWS Firewall Manager e un numero significativo di prodotti di sicurezza di terze parti disponibili in AWS Marketplace nonché il tuo codice, se è stato compilato in modo adeguato. Sia GuardDuty sia Security Hub hanno un modello master-membro che può aggregare risultati e informazioni su più account. Inoltre, Security Hub viene spesso utilizzato dai clienti che dispongono di un sistema SIEM in locale, come un preprocessore e aggregatore di avvisi e log lato AWS, da cui possono quindi acquisire Amazon EventBridge tramite un processore e un server di inoltro basati su Lambda.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle attuali raccomandazioni AWS per l'acquisizione e l'analisi dei log.

Video

- Threat management in the cloud: Amazon GuardDuty & AWS Security Hub
- Centrally Monitoring Resource Configuration & Compliance

Documentazione

- Configurazione di Amazon GuardDuty
- AWS Security Hub
- Nozioni di base su Amazon CloudWatch Logs
- Amazon EventBridge
- Configurazione di Athena per analizzare i log CloudTrail
- Amazon CloudWatch
- AWS Config

- Creazione di un trail in CloudTrail
- Centralize logging solution

Laboratori pratici

- Laboratorio: Enable Security Hub
- Laboratorio: Automated Deployment of Detective Controls
- Laboratorio: Amazon GuardDuty hands on

Analisi

Implementazione di eventi di sicurezza fruibili: per ogni meccanismo di rilevamento di cui disponi, devi disporre anche di un processo, sotto forma di runbook o playbook, da analizzare. Ad esempio, quando abiliti Amazon GuardDuty, vengono generati risultati diversi. È necessario disporre di una voce del runbook per ogni tipo di risultato; ad esempio, se viene rilevato un trojan il runbook contiene istruzioni semplici che indicano come eseguire l'analisi e correggere il problema.

Automatizzazione della risposta agli eventi: in AWS, è possibile analizzare gli eventi di interesse e le informazioni relative alle modifiche potenzialmente impreviste in un flusso di lavoro automatizzato utilizzando Amazon EventBridge. Questo servizio fornisce un motore di regole scalabile progettato per gestire sia i formati di eventi AWS nativi (ad esempio eventi CloudTrail), che gli eventi personalizzati che puoi generare dalla tua applicazione. Amazon EventBridge consente inoltre di instradare gli eventi a un sistema di flusso di lavoro per i sistemi di risposta agli incidenti (Step Functions), a un account di sicurezza centrale o a un bucket per ulteriori analisi.

È inoltre possibile rilevare le modifiche e instradare queste informazioni al flusso di lavoro corretto utilizzando le regole di AWS Config. AWS Config rileva le modifiche apportate ai servizi coperti (anche se con una latenza maggiore rispetto ad Amazon EventBridge) e genera eventi che possono essere analizzati utilizzando le regole di AWS Config per il rollback, l'applicazione delle policy di conformità e l'inoltro di informazioni ai sistemi, quali piattaforme di gestione delle modifiche e sistemi di ticketing operativi. Oltre a scrivere funzioni Lambda personalizzate per rispondere agli eventi di AWS Config, puoi utilizzare il kit per lo sviluppo di regole di AWS Config e una libreria di regole open source di AWS Config.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle attuali best practice di AWS per l'integrazione dei controlli di audit con notifiche e flussi di lavoro.

Video

- Amazon Detective
- Remediating Amazon GuardDuty and AWS Security Hub Findings
- Best Practices for Managing Security Operations on AWS
- Achieving Continuous Compliance using AWS Config

Documentazione

- Amazon Detective
- Amazon EventBridge
- Regole di AWS Config
- AWS Config Rules Repository (open source)
- AWS Config Rules Development Kit

Laboratori pratici

- Soluzione: Real-Time Insights on AWS Account Activity
- Soluzione: Centralized Logging

Protezione dell'infrastruttura

La protezione dell'infrastruttura include metodologie di controllo, ad esempio la difesa avanzata, necessarie per soddisfare le best practice e gli obblighi normativi od organizzativi. L'utilizzo di queste metodologie è fondamentale per il successo delle operazioni continuative nel cloud.

La protezione dell'infrastruttura è una parte fondamentale di un programma di sicurezza delle informazioni. Assicura infatti che i sistemi e i servizi all'interno del carico di lavoro siano protetti contro gli accessi non intenzionali e non autorizzati e contro le potenziali vulnerabilità. Ad esempio, definirai dei limiti di attendibilità (quali i limiti di rete e account), la configurazione e la manutenzione della sicurezza del sistema (includendo argomenti come protezione avanzata, minimizzazione e applicazione di patch), l'autenticazione e le autorizzazioni del sistema operativo (prendendoti cura di utenti, chiavi e livelli di accesso) e altri punti appropriati di applicazione delle policy (quali firewall di applicazioni Web e/o gateway API).

In AWS, ci sono diversi approcci alla protezione dell'infrastruttura. Le seguenti sezioni descrivono come utilizzare questi approcci:

- Protezione delle reti
- Protezione delle risorse di calcolo

Protezione delle reti

L'attenta pianificazione e la gestione della progettazione della rete costituiscono la base del modo in cui fornisci isolamento e limiti per le risorse all'interno del carico di lavoro. Poiché molte risorse nel carico di lavoro operano in un VPC ed ereditano le proprietà di sicurezza, è fondamentale che la progettazione sia supportata da meccanismi di ispezione e protezione supportati dall'automazione. Analogamente, per i carichi di lavoro che operano al di fuori di un VPC, utilizzando esclusivamente servizi edge e/o serverless, le best practice si applicano in un approccio più semplificato. Consulta il documento AWS Well-Architected Serverless Applications Lens per istruzioni specifiche sulla sicurezza serverless.

Creazione di livelli di rete: componenti come istanze EC2, cluster di database RDS e funzioni Lambda che condividono i requisiti di raggiungibilità possono essere segmentati in livelli formati da sottoreti. Ad esempio, un cluster di database RDS in un VPC senza necessità di accesso a Internet deve essere posizionato in sottoreti senza routing da o verso Internet. Questo approccio a più livelli per i controlli mitiga l'impatto di una configurazione errata di un livello singolo, che potrebbe consentire l'accesso involontario. Per AWS Lambda, è possibile eseguire le funzioni nel VPC per anticipare i controlli basati su VPC.

Per la connettività di rete che può includere migliaia di VPC, account AWS e reti locali, è consigliabile utilizzare AWS Transit Gateway. Funge da hub che controlla il modo in cui il traffico viene instradato tra tutte le reti connesse, che agiscono come raggi. Il traffico tra Amazon VPC e AWS Transit Gateway rimane sulla rete privata AWS, riducendo i vettori di minacce esterni, ad esempio attacchi DDoS (Distributed Denial of Service) ed exploit comuni, come SQL injection, script tra siti, richieste tra siti false o uso illecito del codice di autenticazione. Il peering interregionale di AWS Transit Gateway crittografa inoltre il traffico tra regioni senza un singolo punto di errore o collo di bottiglia della larghezza di banda.

Controllo del traffico a tutti i livelli: durante la progettazione della topologia di rete, è necessario esaminare i requisiti di connettività di ciascun componente. Ad esempio, va esaminato se un componente richiede accessibilità a Internet (in entrata e in uscita), connettività a VPC, servizi edge e data center esterni.

Un VPC consente di definire la topologia di rete che si estende su una regione AWS con un intervallo di indirizzi IPv4 privati impostato dall'utente o un intervallo di indirizzi IPv6 selezionato da AWS. È necessario applicare più controlli con un approccio di difesa avanzata sia per il traffico in entrata che per quello in uscita, tra cui l'uso di gruppi di sicurezza (firewall di ispezione stateful), liste di controllo degli accessi di rete, sottoreti e tabelle di routing. All'interno di un VPC, puoi creare sottoreti in una zona di disponibilità. Ogni sottorete può avere una tabella di routing associata che definisce le regole di instradamento per la gestione dei percorsi del traffico all'interno della sottorete. Puoi definire una sottorete Internet instradabile tramite un percorso che va a un gateway Internet o NAT collegato al VPC o attraverso un altro VPC.

Un'istanza, un database RDS o un altro servizio che viene avviato all'interno di un VPC ha un proprio gruppo di sicurezza per interfaccia di rete. Questo firewall è esterno al livello del sistema operativo e può essere utilizzato per definire le regole per il traffico consentito in entrata e in uscita. Puoi anche definire le relazioni tra i gruppi di sicurezza. Ad esempio, le istanze all'interno di un gruppo di sicurezza a livello di database accettano solo il traffico dalle istanze all'interno del livello dell'applicazione, in riferimento ai gruppi di sicurezza applicati alle istanze coinvolte. A meno che non utilizzi protocolli non TCP, non dovrebbe essere necessario disporre di un'istanza EC2 accessibile direttamente da Internet (anche con porte limitate da gruppi di sicurezza) senza un sistema di bilanciamento del carico o CloudFront. Questo aiuta a proteggerla da accessi non intenzionali dovuti a un problema del sistema operativo o dell'applicazione. Una sottorete può anche avere una lista di controllo degli accessi di rete collegata, che funge da firewall stateless. È necessario configurare la lista di controllo degli accessi di rete per limitare l'ambito del traffico consentito tra i livelli; tieni presente che è necessario definire le regole sia in entrata che in uscita.

Mentre alcuni servizi AWS necessitano di componenti per accedere a Internet ed effettuare chiamate API (è qui che si trovano gli endpoint API di AWS) altri utilizzano gli endpoint all'interno dei VPC. Molti servizi AWS, tra cui Amazon S3 e DynamoDB supportano gli endpoint VPC e questa tecnologia è stata generalizzata in AWS PrivateLink. Per gli asset del VPC che devono effettuare connessioni in uscita a Internet, queste possono essere effettuate solo in uscita (unidirezionale) tramite un gateway NAT gestito da AWS, un Internet gateway per connessioni solo in uscita o proxy Web creati e gestiti dall'utente.

Implementazione di attività di ispezione e protezione: ispeziona e filtra il traffico a ogni livello. Per i componenti che eseguono transazioni tramite protocolli basati su HTTP, un firewall per applicazioni Web può aiutare a proteggere dagli attacchi comuni. AWS WAF è un firewall per applicazioni Web che consente di monitorare e bloccare le richieste HTTP che corrispondono alle regole configurabili inoltrate a un'API di Amazon API Gateway, ad Amazon CloudFront o ad Application Load Balancer. Per iniziare a usare AWS WAF, puoi utilizzare le regole gestite di AWS in combinazione con le tue oppure puoi utilizzare integrazioni dei partner esistenti.

Per gestire le protezioni di AWS WAF, AWS Shield Advanced e i gruppi di sicurezza di Amazon VPC in AWS Organizations, puoi utilizzare AWS Firewall Manager. Questo consente di configurare e gestire centralmente le regole del firewall tra gli account e le applicazioni, rendendo più semplice il dimensionamento dell'applicazione delle regole comuni. Consente inoltre di rispondere rapidamente agli attacchi utilizzando AWS Shield Advanced o soluzioni che bloccano automaticamente le richieste indesiderate alle applicazioni Web.

Automatizzazione della protezione di rete: automatizza i meccanismi di protezione per fornire una rete in grado di difendersi da sola sulla base dell'intelligence delle minacce e del rilevamento delle anomalie. Ad esempio, strumenti di rilevamento e prevenzione delle intrusioni in grado di adattarsi alle minacce attuali e di ridurre il loro impatto. Un firewall per applicazioni Web è un esempio di dove è possibile automatizzare la protezione della rete,

ad esempio utilizzando la soluzione Automatismi di sicurezza di AWS WAF (https://github.com/awslabs/aws-waf-security-automations) per bloccare automaticamente le richieste provenienti da indirizzi IP associati a noti attori di minacce.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle best practice di AWS per la protezione delle reti.

Video

- AWS Transit Gateway reference architectures for many VPCs
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield
- DDoS Attack Detection at Scale

Documentazione

- Documentazione di Amazon VPC
- Nozioni di base su AWS WAF
- Liste di controllo accessi di rete
- Gruppi di sicurezza per il VPC
- Regole network ACL consigliate per il tuo VPC
- AWS Firewall Manager
- AWS PrivateLink
- Endpoint VPC
- Amazon Inspector

Laboratori pratici

- Laboratorio: Automated Deployment of VPC
- Laboratorio: Automated Deployment of Web Application Firewall

Protezione delle risorse di calcolo

Gestione delle vulnerabilità: scansiona e aggiungi frequentemente patch contro le vulnerabilità del codice, delle dipendenze e dell'infrastruttura per proteggere da nuove minacce.

Molti aspetti della gestione delle vulnerabilità possono essere automatizzati utilizzando una pipeline di compilazione e distribuzione:

- Utilizzo di strumenti di analisi del codice statico di terze parti per identificare problemi di sicurezza comuni, ad esempio limiti di input delle funzioni non controllati e CVE più recenti. Puoi utilizzare Amazon CodeGuru per le lingue supportate.
- Utilizzo di strumenti di controllo delle dipendenze di terze parti per determinare se le librerie a cui si collega il codice siano le versioni più recenti, se le stesse siano prive di CVE e se le condizioni di licenza soddisfano i requisiti delle policy del software.
- Con Amazon Inspector puoi eseguire valutazioni della configurazione a fronte delle istanze per individuare vulnerabilità ed esposizioni comuni (CVE) note, valutare i valori di riferimento di sicurezza e automatizzare completamente la notifica dei difetti. Amazon Inspector viene eseguito sulle istanze di produzione o in una pipeline e invia una notifica agli sviluppatori e agli ingegneri quando sono disponibili nuovi risultati. Puoi accedere in modo programmatico ai risultati e indirizzare i tuoi team ai sistemi di backlog e rilevamento dei bug. EC2 Image Builder può essere utilizzato per mantenere le immagini del server (AMI) tramite l'applicazione di patch automatizzata, l'applicazione di policy di sicurezza fornite da AWS e altre personalizzazioni.
- Quando utilizzi i container, implementa la scansione delle immagini ECR nella pipeline di compilazione regolarmente confrontandola con il repository di immagini per cercare le CVE nei container.
- Anche se Amazon Inspector e altri strumenti sono efficaci per identificare configurazioni ed eventuali CVE presenti, sono necessari altri metodi per testare il carico di lavoro a livello di applicazione. Ilfuzzing è un metodo noto di individuazione dei bug mediante l'automazione per inserire dati malformati nei campi di input e in altre aree dell'applicazione.

Alcune di queste funzioni possono essere eseguite utilizzando i servizi AWS, i prodotti in AWS Marketplace o gli strumenti open source.

Riduzione della superficie di attacco: riduci la superficie di attacco attraverso la protezione avanzata dei sistemi operativi e riducendo al minimo i componenti, le librerie e i servizi di consumo esterni in uso. Per ridurre la superficie di attacco, è necessario disporre di un modello di rischio per identificare i punti di ingresso e le potenziali minacce che potrebbero essere riscontrate. Una pratica comune per ridurre la superficie di attacco consiste nel ridurre i componenti inutilizzati, siano essi pacchetti del sistema operativo, applicazioni, e così via (per carichi di lavoro basati su EC2) o moduli software esterni nel codice (per tutti i carichi di lavoro). Esistono molte guide per la configurazione della protezione avanzata e della sicurezza dei sistemi operativi e dei software dei server comuni, ad esempio dal Center for Internet Security che puoi utilizzare come punto di partenza e iterazione.

Esecuzione di azioni a distanza: eliminare la possibilità di accesso interattivo riduce il rischio di errore umano e la potenziale configurazione o gestione manuale. Ad esempio, utilizza un flusso di lavoro per la gestione delle modifiche per gestire le istanze EC2 utilizzando strumenti come AWS Systems Manager invece di consentire l'accesso diretto o tramite un bastion host. AWS Systems Manager può automatizzare un'ampia gamma di attività di manutenzione e distribuzione utilizzando funzionalità quali flussi di lavoro di automazione, documenti (playbook) e il run command. Gli stack di AWS CloudFormation si basano su pipeline e possono automatizzare le attività di distribuzione e gestione dell'infrastruttura senza utilizzare direttamente la Console di gestione AWS o le API.

Implementazione di servizi gestiti: implementa servizi che gestiscono le risorse, ad esempio Amazon RDS, AWS Lambda e Amazon ECS, per ridurre le attività di manutenzione della sicurezza nell'ambito del modello di responsabilità condivisa. Ad esempio, Amazon RDS aiuta a configurare, gestire e dimensionare un database relazionale e automatizza le attività di amministrazione quali provisioning di hardware, configurazione di database, applicazione di patch e backup. Ciò significa che hai più tempo libero per concentrarti sulla protezione dell'applicazione in altri modi descritti nel Canone di architettura AWS. AWS Lambda consente di eseguire il codice senza dover effettuare il provisioning o gestire server, perciò è sufficiente focalizzarsi su connettività, invocazione e sicurezza a livello di codice piuttosto che sull'infrastruttura o il sistema operativo.

Convalida dell'integrità del software: implementa meccanismi (ad esempio la firma del codice) per convalidare che il software, il codice e le librerie utilizzati nel carico di lavoro provengano da origini attendibili e non siano stati manomessi. Ad esempio, devi verificare il certificato di firma del codice dei file binari e degli script per confermare l'autore e accertarti che non sia stato manomesso da quando è stato creato dall'autore. Inoltre, un confronto tra il checksum del software scaricato e quello del provider può garantire che non sia stato manomesso.

Automatizzazione della protezione delle risorse di calcolo: automatizza i meccanismi di protezione delle risorse di calcolo, tra cui la gestione delle vulnerabilità, la riduzione della superficie di attacco e la gestione delle risorse. L'automazione ti consentirà di investire tempo nella protezione di altri aspetti del carico di lavoro e di ridurre il rischio di errori umani.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle best practice di AWS per la protezione delle risorse di calcolo.

Video

- Security best practices for the Amazon EC2 instance metadata service
- Securing Your Block Storage on AWS
- Securing Serverless and Container Services

- Running high-security workloads on Amazon EKS
- Architecting Security through Policy Guardrails in Amazon EKS

Documentazione

- Security Overview of AWS Lambda
- Sicurezza in Amazon EC2
- AWS Systems Manager
- Amazon Inspector
- Writing your own AWS Systems Manager documents
- Replacing a Bastion Host with Amazon EC2 Systems Manager

Laboratori pratici

- Laboratorio: Automated Deployment of EC2 Web Application

Protezione dei dati

Prima di progettare qualsiasi carico di lavoro, dovrebbero essere messe in atto pratiche fondamentali che influenzano la sicurezza. Ad esempio, la classificazione dei dati fornisce un modo per categorizzare i dati in base ai livelli di sensibilità mentre la crittografia protegge i dati rendendoli incomprensibili agli accessi non autorizzati. Questi metodi sono importanti perché supportano obiettivi quali la prevenzione di una gestione errata o la conformità agli obblighi normativi.

In AWS, è possibile utilizzare diversi approcci per la protezione dei dati. La seguente sezione descrive come utilizzare questi approcci:

- Classificazione dei dati
- Protezione dei dati inattivi
- Protezione dei dati in transito

Classificazione dei dati

La classificazione dei dati fornisce un modo per categorizzare i dati dell'organizzazione in base ai livelli di criticità e sensibilità, in modo da aiutarti a determinare i controlli di protezione e conservazione appropriati.

Identificazione dei dati all'interno del carico di lavoro: è necessario comprendere il tipo e la classificazione dei dati elaborati dal carico di lavoro, i processi aziendali associati, il proprietario dei dati, i requisiti legali e di conformità applicabili, il luogo di archiviazione e i controlli risultanti da applicare. Ciò può includere classificazioni per indicare se i dati sono destinati a essere disponibili al pubblico, se i dati sono solo di uso interno, ad esempio informazioni che consentono l'identificazione personale del cliente (PII, Personally Identifiable Information), oppure se i dati riguardano un accesso più limitato, ad esempio relativi alla proprietà intellettuale, dati confidenziali o sensibili e altro ancora. L'attenta gestione di un sistema appropriato di classificazione dei dati e dei requisiti di protezione di ciascun livello del carico di lavoro consente di mappare i controlli e il livello di accesso/protezione dei dati adeguato. Ad esempio, i contenuti destinati al pubblico sono accessibili a tutti, ma i contenuti importanti sono crittografati e archiviati in modo protetto e richiedono l'accesso autorizzato a una chiave per essere decrittati.

Definizione dei controlli per la protezione dei dati: utilizzando tag di risorse, account AWS separati per livelli di sensibilità (e potenzialmente anche per avvertimento/enclave/community di interesse), policy IAM, SCP di AWS Organizations, AWS KMS e AWS CloudHSM, puoi definire e implementare le policy per la classificazione e la protezione dei dati tramite la crittografia. Ad esempio, se in un progetto sono presenti bucket S3 che contengono dati estremamente critici o istanze EC2 che elaborano dati riservati, essi possono essere contrassegnati con un tag

"Progetto=ABC". Solo il team ristretto conosce il significato del codice del progetto e rappresenta un modo per utilizzare il controllo degli accessi basato su attributi. Puoi definire i livelli di accesso alle chiavi di crittografia AWS KMS tramite policy e concessioni delle chiavi per garantire che solo i servizi appropriati abbiano accesso ai contenuti sensibili tramite un meccanismo sicuro. Se prendi decisioni in merito alle autorizzazioni in base ai tag, devi assicurarti che le autorizzazioni sui tag siano definite in modo appropriato utilizzando le policy dei tag in AWS Organizations.

Definizione della gestione del ciclo di vita dei dati: la strategia del ciclo di vita definita deve basarsi sul livello di sensibilità e sui requisiti legali e aziendali. Gli aspetti da considerare includono la durata di conservazione dei dati, i processi di distruzione dei dati, la gestione degli accessi ai dati, la trasformazione dei dati e la condivisione dei dati. Nella scelta di una metodologia di classificazione dei dati, è necessario valutare l'usabilità rispetto all'accesso. Devi inoltre gestire vari livelli di accesso e particolarità per implementare un approccio sicuro e utilizzabile per ogni livello. Utilizza sempre un approccio di difesa avanzata e riduci l'accesso umano ai dati e ai meccanismi per trasformare, eliminare o copiare i dati. Ad esempio, richiedi agli utenti di effettuare l'autenticazione in un'applicazione e fornisci all'applicazione, anziché agli utenti, l'autorizzazione di accesso necessaria per eseguire "operazioni a distanza". Inoltre, assicurati che gli utenti provengano da un percorso di rete sicuro e richiedi l'accesso alle chiavi di decrittografia. Utilizza strumenti, pannelli di controllo e generazione di report automatizzata, per fornire agli utenti informazioni ricavate dai dati piuttosto che concedere loro l'accesso diretto ai dati.

Automatizzazione dell'identificazione e della classificazione: automatizzare l'identificazione e la classificazione dei dati può aiutarti a implementare i controlli corretti. L'utilizzo dell'automazione per queste operazioni invece dell'accesso diretto da parte di una persona riduce il rischio di errori umani e di esposizione delle persone. È consigliabile valutare l'utilizzo di uno strumento, ad esempio Amazon Macie, che utilizza il machine learning per rilevare, classificare e proteggere automaticamente i dati sensibili in AWS. Amazon Macie riconosce i dati sensibili, quali informazioni personali o di proprietà intellettuale e fornisce pannelli di controllo e allarmi che offrono visibilità su come viene effettuato l'accesso a tali dati o come vengono spostati.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulla classificazione dei dati.

Documentazione

- Whitepaper sulla classificazione dei dati
- Tagging delle risorse Amazon EC2
- Tagging degli oggetti di Amazon S3

Protezione dei dati inattivi

I dati inattivi rappresentano tutti i dati conservati nello storage non volatile per qualsiasi durata del carico di lavoro. Sono inclusi storage a blocchi, storage di oggetti, database, archivi, dispositivi IoT e qualsiasi altro supporto di storage su cui sono conservati i dati. La protezione dei dati inattivi riduce il rischio di accesso non autorizzato quando vengono implementati crittografia e controlli degli accessi adeguati.

La crittografia e la tokenizzazione sono due metodi di protezione dei dati importanti ma distinti.

La*tokenizzazione* è un processo che consente di definire un token per rappresentare un'informazione altrimenti sensibile (ad esempio, un token per rappresentare il numero di carta di credito di un cliente). Un token deve essere privo di significato e non deve derivare dai dati che sta tokenizzando; pertanto, un digest crittografico non è utilizzabile come token. Pianificando attentamente l'approccio alla tokenizzazione, puoi fornire una protezione aggiuntiva ai contenuti e assicurarti di soddisfare i requisiti di conformità. Ad esempio, puoi limitare l'ambito di conformità di un sistema di elaborazione delle carte di credito se utilizzi un token anziché un numero di carta di credito.

La crittografia è un sistema per trasformare i contenuti in modo da renderli illeggibili senza una chiave segreta necessaria per decrittare di nuovo i contenuti in testo normale. Sia la tokenizzazione che la crittografia possono essere utilizzate per mettere in sicurezza e proteggere le informazioni nel modo più adeguato. Inoltre, il mascheramento è una tecnica che consente di redigere una parte di dati fino a un punto in cui i dati rimanenti non sono considerati sensibili. Ad esempio, PCI-DSS consente di conservare le ultime quattro cifre di un numero di carta fuori dal limite dell'ambito di conformità per l'indicizzazione.

Implementazione della gestione sicura delle chiavi: definendo un approccio alla crittografia che include lo storage, la rotazione e il controllo degli accessi delle chiavi, puoi contribuire a proteggere i tuoi contenuti da utenti non autorizzati e dall'esposizione non necessaria agli utenti autorizzati. AWS KMS ti aiuta a gestire le chiavi di crittografia e si integra con molti servizi AWS. Si tratta di un servizio che fornisce uno storage durevole, sicuro e ridondante per le tue chiavi master. Puoi definire i tuoi alias delle chiavi e le policy a livello di chiave. Le policy ti aiutano a definire gli amministratori della chiave e i suoi utenti. Inoltre, AWS CloudHSM è un modulo di sicurezza hardware (HSM, Hardware Security Module) basato sul cloud che consente di generare e utilizzare chiavi di crittografia personalizzate in AWS Cloud. Ti aiuta a rispettare i requisiti di conformità aziendali, contrattuali e normativi per la sicurezza dei dati utilizzando HSM conformi allo standard FIPS 140-2 Level 3.

Applicazione della crittografia dei dati inattivi: devi accertarti che l'unico modo per archiviare i dati sia l'utilizzo della crittografia. AWS KMS si integra perfettamente con molti servizi AWS per semplificare la crittografia di tutti i dati inattivi. Ad esempio, in Amazon S3 puoi impostare la crittografia predefinita su un bucket in modo che tutti nuovi oggetti vengano crittografati automaticamente. Inoltre, Amazon EC2 supporta l'applicazione della crittografia impostando un'opzione di crittografia predefinita per un'intera regione.

Applicazione del controllo degli accessi: diversi controlli, tra cui accesso (con privilegi minimi), backup (consulta il whitepaper sull'affidabilità), isolamento e versioning, possono tutti aiutare a proteggere i dati inattivi. L'accesso ai dati deve essere controllato utilizzando i meccanismi di rilevamento trattati in precedenza in questo documento, tra cui CloudTrail e il log del livello di servizio, ad esempio i log di accesso S3. Devi eseguire un inventario dei dati accessibili al pubblico e pianificare come ridurre la quantità di dati disponibili nel tempo. Amazon S3 Glacier Vault Lock e S3 Object Lock sono funzionalità che forniscono un controllo degli accessi obbligatorio. Una volta bloccata una policy Vault con l'opzione di conformità, nemmeno l'utente root può modificarla fino alla scadenza del blocco. Il meccanismo soddisfa i requisiti di gestione di libri e record di SEC, CFTC e FINRA. Per ulteriori dettagli, consulta questo whitepaper.

Audit dell'utilizzo delle chiavi di crittografia: assicurati di comprendere e controllare l'uso delle chiavi di crittografia per convalidare che i meccanismi di controllo degli accessi sulle chiavi siano implementati in modo appropriato. Ad esempio, qualsiasi servizio AWS che utilizzi una chiave AWS KMS registra ogni utilizzo in AWS CloudTrail. Puoi quindi eseguire query ad AWS CloudTrail utilizzando uno strumento come Amazon CloudWatch Insights, per assicurarti che tutti gli utilizzi delle chiavi siano validi.

Utilizzo di meccanismi per evitare l'accesso delle persone ai dati: evita a tutti gli utenti di accedere direttamente a dati e sistemi sensibili in circostanze operative normali. Ad esempio, usa un flusso di lavoro per la gestione delle modifiche per gestire le istanze EC2 tramite strumenti, invece di consentire l'accesso diretto o tramite un bastion host. A tal fine puoi utilizzare AWS Systems Manager Automation, che utilizza documenti di automazione che contengono le fasi utilizzate per eseguire le attività. Questi documenti possono essere archiviati nel controllo sorgente, revisionati in peering prima dell'esecuzione e testati accuratamente per ridurre al minimo i rischi rispetto all'accesso alla shell. Gli utenti aziendali possono utilizzare un pannello di controllo anziché accedere direttamente a un datastore per eseguire query. Se non vengono utilizzate le pipeline CI/CD, determina quali controlli e processi sono necessari per fornire in modo adeguato un meccanismo di accesso di tipo break-glass normalmente disabilitato.

Automatizzazione della protezione dei dati inattivi: utilizza strumenti automatizzati per convalidare e applicare i controlli dei dati inattivi in modo continuo; ad esempio verifica che siano presenti solo risorse di storage crittografate. Puoi automatizzare la convalida della crittografia di tutti i volumi EBS utilizzando le regole di AWS Config. AWS Security Hub può anche verificare una serie di controlli diversi tramite controlli automatici a fronte di standard di sicurezza. Inoltre, le regole di AWS Config possono correggere automaticamente le risorse non conformi.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle best practice di AWS per la protezione dei dati inattivi.

Video

- How Encryption Works in AWS
- Securing Your Block Storage on AWS
- Achieving security goals with AWS CloudHSM
- Best Practices for Implementing AWS Key Management Service
- A Deep Dive into AWS Encryption Services

Documentazione

- Protezione dei dati di Amazon S3 tramite la crittografia
- Crittografia di Amazon EBS
- Crittografia delle risorse di Amazon RDS
- Protezione dei dati tramite la crittografia
- In che modo i servizi AWS utilizzano AWS KMS
- Crittografia di Amazon EBS
- AWS Key Management Service
- AWS CloudHSM
- Whitepaper sui dettagli della crittografia di AWS KMS
- Utilizzo delle policy delle chiavi in AWS KMS
- Utilizzo delle policy di bucket e delle policy utente
- AWS Crypto Tools

Protezione dei dati in transito

I dati in transito sono tutti i dati inviati da un sistema a un altro. Ciò include la comunicazione tra le risorse all'interno del carico di lavoro e la comunicazione tra altri servizi e gli utenti finali. Fornendo il livello di protezione appropriato per i dati in transito, proteggi la riservatezza e l'integrità dei dati del carico di lavoro.

Implementazione della gestione sicura delle chiavi e dei certificati: archivia le chiavi di crittografia e i certificati in modo sicuro e ruotali a intervalli di tempo appropriati tramite un controllo rigoroso degli accessi. Il modo migliore per farlo è utilizzare un servizio gestito, ad esempio AWS Certificate Manager (ACM). Questo servizio consente di effettuare il provisioning, gestire e distribuire facilmente certificati TLS (Transport Layer Security) pubblici e privati da utilizzare con i servizi AWS e le risorse interne connesse. I certificati TLS vengono utilizzati per proteggere le comunicazioni di rete e stabilire l'identità dei siti Web su Internet e delle risorse su reti private. ACM si integra con le risorse AWS, ad esempio Elastic Load Balancer, distribuzioni Amazon CloudFront e API su API Gateway, gestendo anche rinnovi automatici dei certificati. Se utilizzi ACM per distribuire un'autorità di certificazione (CA, Certificate Authority) root privata, esso può fornire sia certificati che chiavi private da utilizzare in istanze EC2, container e così via.

Applicazione della crittografia in transito: applica i tuoi requisiti di crittografia definiti in base ad appropriati standard e raccomandazioni in modo da soddisfare i requisiti aziendali, legali e di conformità. I servizi AWS forniscono endpoint HTTPS utilizzando TLS per le comunicazioni e pertanto forniscono crittografia in transito quando comunicano con le API AWS. I protocolli non sicuri, come HTTP, possono essere controllati e bloccati in un VPC tramite l'uso di gruppi di sicurezza. Le richieste HTTP possono anche essere reindirizzate automaticamente HTTPS in Amazon CloudFront o in un Application Load Balancer. Hai il controllo completo sulle tue risorse informatiche per implementare la crittografia in transito nei tuoi servizi. Inoltre, puoi utilizzare la connettività VPN nel VPC da una rete esterna per facilitare la crittografia del traffico. Per requisiti particolari, in AWS Marketplace sono disponibili soluzioni di terze parti.

Autenticazione delle comunicazioni di rete: l'utilizzo di protocolli di rete che supportano l'autenticazione consente di stabilire l'attendibilità tra le parti. Questo si aggiunge alla crittografia utilizzata nel protocollo per ridurre il rischio che le comunicazioni vengano alterate o intercettate. I protocolli comuni che implementano l'autenticazione includono il protocollo TLS (Transport Layer Security), che viene utilizzato in molti servizi AWS, e IPsec, utilizzato in AWS Virtual Private Network (AWS VPN).

Rilevamento automatico degli accessi non intenzionali ai dati: utilizza strumenti come Amazon GuardDuty per rilevare automaticamente i tentativi di spostamento dei dati al di fuori di limiti definiti in base al livello di classificazione dei dati, ad esempio per rilevare un trojan che sta copiando i dati in una rete sconosciuta o non attendibile utilizzando il protocollo DNS. Oltre ad Amazon GuardDuty, si possono utilizzare i log di flusso di Amazon VPC, che acquisiscono informazioni sul traffico di rete, con Amazon EventBridge per attivare il rilevamento di connessioni anomale, riuscite e negate. S3 Access Analyzer può aiutare a valutare quali dati sono accessibili a chi nei bucket S3.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle best practice AWS per la protezione dei dati in transito.

Video

- How can I add certificates for websites to the ELB using AWS Certificate Manager
- Deep Dive on AWS Certificate Manager Private CA

Documentazione

- AWS Certificate Manager
- Listener HTTPS per Application Load Balancer
- AWS VPN
- API Gateway ottimizzato per edge

Risposta agli incidenti

Anche se dispone di controlli preventivi e di rilevamento estremamente maturi, l'organizzazione deve ancora implementare meccanismi per rispondere e mitigare il potenziale impatto degli incidenti di sicurezza. La tua preparazione influisce fortemente sulla capacità dei team di operare in modo efficace durante un incidente, isolare e contenere i problemi e ripristinare le operazioni a uno stato valido noto. La messa in atto degli strumenti e l'accesso prima di un incidente di sicurezza, quindi la pratica sistematica della risposta agli incidenti durante le giornate di gioco, aiuterà a garantire il ripristino, riducendo al minimo le interruzioni dell'attività.

Progettazione degli obiettivi di risposta al cloud

Sebbene i processi e i meccanismi generali di risposta agli incidenti, come quelli definiti nella NIST SP 800-61 Computer Security Incident Handling Guide, rimangano validi, ti consigliamo di valutare i seguenti obiettivi di progettazione specifici pertinenti per rispondere agli incidenti di sicurezza in un ambiente cloud:

- **Definizione degli obiettivi di risposta:** collabora con le parti interessate, i consulenti legali e la leadership dell'organizzazione per determinare l'obiettivo di risposta a un incidente. Alcuni obiettivi comuni includono il contenimento e la mitigazione del problema, il ripristino delle risorse interessate, la conservazione dei dati per le analisi forensi e l'attribuzione.
- **Piani dei documenti:** crea piani che ti aiutino a rispondere, comunicare durante ed effettuare il ripristino dopo un incidente.
- **Risposte fornite utilizzando il cloud:** implementa i tuoi modelli di risposta dove si verificano l'evento e i dati.
- **Individuazione dei dati esistenti e di quelli necessari:** conserva log, snapshot e altre prove copiandoli in un account cloud di sicurezza centralizzato. Utilizza tag, metadati e meccanismi che applicano le policy di conservazione. Ad esempio, puoi scegliere di utilizzare il comando `dd` di Linux o un equivalente di Windows per creare una copia completa dei dati a scopo investigativo.
- **Utilizzo di meccanismi di ridistribuzione:** se un'anomalia di sicurezza può essere attribuita a una configurazione errata, la correzione potrebbe essere semplicemente rimuovere la varianza ridistribuendo le risorse con la configurazione corretta. Quando possibile, rendi i meccanismi di risposta sicuri in modo da eseguirli più di una volta e in ambienti in uno stato sconosciuto.

- **Automatizzazione laddove possibile:** quando si verificano problemi o incidenti ripetuti, crea meccanismi che verifichino e rispondano a situazioni comuni a livello di programmazione. Utilizza le risposte umane per incidenti unici, nuovi e sensibili.
- **Scelta di soluzioni scalabili:** cerca di soddisfare la scalabilità dell'approccio aziendale al cloud computing e riduci le tempistiche tra rilevamento e risposta.
- **Individuazione delle lacune e miglioramento del processo:** quando individui lacune nel processo, negli strumenti o nelle persone, implementa piani per correggerle. Le simulazioni sono metodi sicuri per individuare le lacune e migliorare i processi.

In AWS, è possibile utilizzare diversi approcci per rispondere agli incidenti. La seguente sezione descrive come utilizzare questi approcci:

- **Istruzione** del personale che si occupa delle operazioni di sicurezza e della risposta agli incidenti in merito alle tecnologie cloud e al modo in cui l'organizzazione intende utilizzarle.
- **Preparazione** del team di risposta agli incidenti per rilevare e rispondere agli incidenti nel cloud; abilita le funzionalità di rilevamento e assicura l'accesso appropriato agli strumenti e ai servizi cloud necessari. Inoltre, prepara i runbook necessari, sia manuali che automatizzati, per garantire risposte affidabili e coerenti. Collabora con altri team per stabilire le operazioni di base previste e utilizza tali conoscenze per identificare le divergenze rispetto alle operazioni normali.
- **Simulazione** di eventi di sicurezza previsti e imprevisti all'interno dell'ambiente cloud per comprendere l'efficacia della preparazione.
- **Iterazione** sull'esito della simulazione per migliorare la scala di risposta, ridurre il time-to-value e ridurre ulteriormente il rischio.

Istruzione

I processi automatizzati consentono alle organizzazioni di dedicare più tempo a concentrarsi sulle misure per aumentare la sicurezza dei propri carichi di lavoro. La risposta automatizzata agli incidenti offre inoltre più tempo al personale per correlare eventi, eseguire simulazioni, ideare nuove procedure di risposta, eseguire ricerche, sviluppare nuove competenze e testare o creare nuovi strumenti. Nonostante la maggiore automazione, il team, gli specialisti e il personale responsabile della riposta agli incidenti all'interno di un'organizzazione di sicurezza richiedono una formazione continua.

Oltre all'esperienza generale del cloud, per avere successo è necessario investire in modo significativo nel proprio personale. L'organizzazione può trarre vantaggio dalla formazione aggiuntiva del personale per apprendere le competenze di programmazione, i processi di sviluppo (inclusi i sistemi di controllo delle versioni e le pratiche di distribuzione) e l'automazione dell'infrastruttura. Il modo migliore per apprendere è la pratica, attraverso l'organizzazione di game day sulla risposta agli incidenti. In questo modo, gli esperti del team possono affinare gli strumenti e le tecniche mentre insegnano agli altri.

Preparazione

Durante un incidente, i team di risposta agli incidenti devono avere accesso a vari strumenti e alle risorse del carico di lavoro coinvolte nell'incidente. Assicurati che i team dispongano dell'accesso preassegnato appropriato per eseguire le loro attività prima che si verifichi un evento. Tutti gli strumenti, gli accessi e i piani devono essere documentati e testati prima che si verifichi un evento per garantire che i team possano fornire una risposta tempestiva.

Identificazione del personale chiave e delle risorse esterne: quando definisci come affrontare la risposta agli incidenti nel cloud, insieme ad altri team (ad esempio il consulente legale, la leadership dell'organizzazione, le parti interessate, i servizi AWS Support e altri), devi identificare il personale chiave, le parti interessate e i contatti pertinenti. Per ridurre le dipendenze e i tempi di risposta, assicurati che il personale, i team di sicurezza specializzati e i team che rispondono agli incidenti ricevano informazioni sui servizi che utilizzi e abbiano l'opportunità di esercitarsi direttamente.

Ti invitiamo a identificare i partner di sicurezza AWS esterni in grado di fornirti competenze e una prospettiva diversa per potenziare le tue capacità di risposta. I partner di sicurezza affidabili possono aiutarti a identificare potenziali rischi o minacce che potresti non conoscere.

Sviluppo di piani di gestione degli incidenti: crea piani che ti aiutino a rispondere a un incidente, comunicare durante lo stesso e ripristinare in seguito le risorse. Ad esempio, puoi iniziare dal piano di risposta agli incidenti con gli scenari più probabili per il carico di lavoro e l'organizzazione. Includi il modo in cui gestiresti la comunicazione e l'escalation internamente ed esternamente. Crea piani di risposta agli incidenti sotto forma di playbook a partire dagli scenari più probabili per il carico di lavoro e l'organizzazione. Questi potrebbero essere eventi generati attualmente. Se hai bisogno di un punto di partenza, consulta i risultati di AWS Trusted Advisor e Amazon GuardDuty. Utilizza un formato semplice, come Markdown, che è facile da mantenere, ma assicurati che siano inclusi comandi importanti o frammenti di codice in modo che possano essere eseguiti senza dover consultare altra documentazione.

Inizia in modo semplice ed esegui l'iterazione. Collabora a stretto contatto con gli esperti di sicurezza e partner al fine di identificare le attività necessarie per garantire che i processi siano possibili. Definisci le descrizioni manuali dei processi che esegui. Successivamente, testa i processi ed esegui l'iterazione sul modello runbook per migliorare la logica di base della risposta. Determina quali sono le eccezioni e quali sono le risoluzioni alternative per tali scenari. Ad esempio, in un ambiente di sviluppo, potresti voler terminare un'istanza Amazon EC2 configurata in modo errato. Tuttavia, se lo stesso evento si è verificato in un ambiente di produzione, invece di terminare l'istanza puoi arrestare l'istanza e verificare con le parti interessate che i dati critici non andranno persi e che la terminazione sia accettabile. Includi il modo in cui gestiresti la comunicazione e l'escalation internamente ed esternamente. Quando sei a tuo agio con la risposta manuale al processo, automatizzala per ridurre il tempo di risoluzione.

Assegnazione anticipata dell'accesso: assicurati che al team di risposta agli incidenti sia stato preassegnato l'accesso corretto ad AWS e ad altri sistemi pertinenti per ridurre i tempi di verifica fino al ripristino. Determinare come ottenere l'accesso per le persone giuste durante un incidente ritarda il tempo di risposta e può provocare ulteriori vulnerabilità in ambito di sicurezza se l'accesso è condiviso o non è stato effettuato il provisioning in situazioni pressanti. È necessario conoscere il livello di accesso richiesto dai membri del team (ad esempio, quali tipi di azioni potrebbero intraprendere) ed è necessario assegnare l'accesso in anticipo. L'accesso sotto forma di ruoli o utenti creati appositamente per rispondere a un incidente di sicurezza è spesso privilegiato per fornire accesso sufficiente. Pertanto, l'uso di questi account utente deve essere limitato, essi non devono essere utilizzati per le attività quotidiane e devono essere impostati degli avvisi per il relativo utilizzo.

Distribuzione anticipata degli strumenti: assicurati che il personale addetto alla sicurezza disponga degli strumenti giusti pre-distribuiti in AWS per ridurre i tempi di verifica fino al ripristino.

Per automatizzare le funzioni delle operazioni e la progettazione della sicurezza, puoi utilizzare un set completo di API e strumenti di AWS. Puoi automatizzare completamente le funzionalità di gestione delle identità, sicurezza della rete, protezione dei dati e monitoraggio e distribuirle utilizzando metodi di sviluppo software comuni già esistenti. Quando crei l'automazione della sicurezza, il sistema può monitorare, rivedere e avviare una risposta, invece di far monitorare alle persone il comportamento di sicurezza e reagire manualmente agli eventi.

Se i team di risposta agli incidenti continuano a rispondere agli avvisi nello stesso modo, rischiano il cosiddetto affaticamento dagli avvisi ("alert fatigue"). Ciò significa che, nel corso del tempo, il team può diventare desensibilizzato agli avvisi e può commettere errori nella gestione di situazioni ordinarie o farsi sfuggire avvisi insoliti. L'automazione aiuta a evitare l'affaticamento dagli avvisi utilizzando funzioni che elaborano gli avvisi ripetitivi e ordinari, lasciando alle persone la gestione degli incidenti sensibili e univoci.

Puoi migliorare i processi manuali automatizzando le fasi del processo a livello di programmazione. Dopo aver definito il modello di correzione di un evento, puoi decomporre tale modello in una logica fruibile e scrivere il codice per eseguire tale logica. Il team di risposta può quindi eseguire il codice per risolvere il problema. Nel corso del tempo, puoi automatizzare più fasi e, infine, gestire automaticamente intere classi di incidenti comuni.

Per gli strumenti eseguiti all'interno del sistema operativo dell'istanza EC2, considera l'utilizzo di Run Command di AWS Systems Manager, che consente di amministrare le istanze in remoto e in modo sicuro utilizzando un agente installato nel sistema operativo delle istanze Amazon EC2. È richiesto l'agente AWS Systems Manager (Agente SSM), installato per impostazione predefinita su molte Amazon Machine Image (AMI). Tieni presente, tuttavia, che una volta che un'istanza è stata compromessa, nessuna risposta da parte di strumenti o agenti in esecuzione su di essa va considerata affidabile.

Preparazione delle capacità forensi: identifica e prepara le capacità di indagini forensi idonee, tra cui specialisti esterni, strumenti e automazione. Alcune delle attività di risposta agli incidenti potrebbero includere l'analisi di immagini del disco, file system, dump della RAM o altri artefatti coinvolti in un incidente. Crea una workstation forense personalizzata da utilizzare per montare copie di qualsiasi volume di dati interessato. Poiché le tecniche di indagine forensi richiedono una formazione specializzata, potrebbe essere necessario coinvolgere specialisti esterni.

Simulazione

Organizzazione di game day: i game day, noti anche come simulazioni o esercizi, sono eventi interni che offrono un'opportunità strutturata per mettere in pratica i piani e le procedure di gestione degli incidenti in uno scenario realistico. I game day riguardano fondamentalmente la preparazione e il miglioramento iterativo delle capacità di risposta. Alcuni dei motivi per cui potresti trovare utile l'organizzazione di game day includono:

- Convalida della preparazione
- Sviluppo delle competenze: apprendimento da simulazioni e dal personale preposto alla formazione
- Rispetto degli obblighi contrattuali o di conformità
- Generazione di artefatti per l'accreditamento
- Agilità: miglioramento incrementale
- Maggiore rapidità e miglioramento degli strumenti
- Perfezionamento della comunicazione e dell'escalation
- Gestione più sicura delle situazioni rare e inaspettate

Per questi motivi, il valore derivato dalla partecipazione a un'attività SIRS (Security Incident Response Simulation) aumenta l'efficacia di un'organizzazione durante gli eventi stressanti. Sviluppare un'attività SIRS realistica e utile può essere un esercizio difficile. Anche se testare le procedure o l'automazione che gestisce eventi noti presenta alcuni vantaggi, è altrettanto utile partecipare alle attività SIRS creative per mettersi alla prova in situazioni impreviste e migliorare continuamente.

Iterazione

Automatizzazione della capacità di contenimento e di ripristino: automatizza il contenimento e il ripristino di un incidente per ridurre i tempi di risposta e l'impatto sull'organizzazione.

Dopo aver creato e utilizzato i processi e gli strumenti dai playbook, puoi decostruire la logica in una soluzione basata su codice, che può essere utilizzata come strumento dal team di risposta per automatizzare la risposta e rimuovere la varianza o le supposizioni. Questo può accelerare il ciclo di vita di una risposta. L'obiettivo successivo è abilitare questo codice in modo che sia completamente automatizzato e che possa essere richiamato dagli avvisi o dagli eventi stessi, piuttosto che da un addetto alle risposte, per creare una risposta basata sugli eventi.

Tramite un sistema di risposta basata sugli eventi, un meccanismo di rilevamento attiva un meccanismo di risposta per correggere automaticamente l'evento. Puoi utilizzare le funzionalità di risposta basata sugli eventi per ridurre il time-to-value tra meccanismi di rilevamento e di risposta. Per creare questa architettura basata sugli eventi, puoi utilizzare AWS Lambda, un servizio di elaborazione serverless che esegue il codice in risposta a eventi e gestisce automaticamente le risorse di calcolo sottostanti per tuo conto. Ad esempio, supponiamo che tu disponga di un account AWS con il servizio AWS CloudTrail abilitato. Se AWS CloudTrail è disabilitato (tramite la chiamata API `cloudtrail:StopLogging`), puoi utilizzare Amazon EventBridge per monitorare l'evento specifico `cloudtrail:StopLogging` e richiamare una funzione AWS Lambda al fine di chiamare `cloudtrail:StartLogging` per riavviare la registrazione.

Risorse

Consulta le seguenti risorse per ottenere ulteriori informazioni sulle best practice di AWS per la risposta agli incidenti.

Video

- Prepare for & respond to security incidents in your AWS environment
- Automating Incident Response and Forensics
- DIY guide to runbooks, incident reports, and incident response

Documentazione

- AWS Incident Response Guide
- AWS Step Functions
- Amazon EventBridge
- CloudEndure Disaster Recovery

Laboratori pratici

- Laboratorio: Incident Response with AWS Console and CLI
- Laboratorio: Incident Response Playbook with Jupyter - AWS IAM
- Blog: Orchestrating a security incident response with AWS Step Functions

Conclusioni

La sicurezza è un impegno continuo. Quando si verificano incidenti, devono essere trattati come opportunità per migliorare la sicurezza dell'architettura. I controlli di identità avanzati, le risposte automatizzate agli eventi di sicurezza, l'infrastruttura protetta a più livelli e la gestione dei dati ben classificati tramite la crittografia forniscono una difesa avanzata che ogni organizzazione deve implementare. Ciò risulta più semplice grazie alle funzionalità programmatiche e alle caratteristiche e ai servizi AWS discussi in questo documento.

AWS si impegna ad aiutarti a creare e gestire architetture che proteggano informazioni, sistemi e asset offrendo valore aziendale aggiunto.

Collaboratori

Hanno contribuito alla stesura di questo documento:

- Ben Potter, Principal Security Lead, Well-Architected, Amazon Web Services
- Bill Shinn, Senior Principal, Ufficio del CISO, Amazon Web Services
- Brigid Johnson, Senior Software Development Manager, AWS Identity, Amazon Web Services
- Bynes Pogson, Senior Solution Architect, Amazon Web Services
- Darran Boyd, Principal Security Solutions Architect, Servizi finanziari, Amazon Web Services
- Dave Walker, Principal Specialist Solutions Architect, Sicurezza e conformità, Amazon Web Services
- Paul Hawkins, Senior Security Strategist, Amazon Web Services
- Sam Elmalak, Senior Technology Leader, Amazon Web Services

Approfondimenti

Per ulteriore assistenza, consulta le seguenti risorse:

- Whitepaper sul Canone di architettura AWS

Revisioni del documento

Data	Descrizione
Luglio 2020	Linee guida aggiornate sulla gestione di account, identità e autorizzazioni.
Aprile 2020	Aggiornato per ampliare i consigli in ogni area, nuove best practice, servizi e funzionalità.
Luglio 2018	Aggiornamenti che rispecchiano i nuovi servizi e funzionalità di AWS; riferimenti aggiornati.
Maggio 2017	La sezione su configurazione e mantenimento della sicurezza del sistema presenta i nuovi servizi e le nuove funzionalità di AWS.
Novembre 2016	Prima pubblicazione