Pilar de seguridad

Marco de Buena Arquitectura de AWS

Julio de 2020

This paper has been archived.

The latest version is now available at:

https://docs.aws.amazon.com/es_es/wellarchitected/latest/reliability-pillar/welcome.html

Avisos

Los clientes son responsables de hacer su propia evaluación independiente de la información en este documento. Este documento: (a) solo tiene fines informativos, (b) representa las prácticas y las ofertas de productos de AWS actuales, las cuales están sujetas a cambios sin aviso previo, y (c) no crea compromisos ni promesas de parte de AWS y sus empresas afiliadas, proveedores o licenciantes. Los servicios o los productos de AWS se ofrecen “como son”, sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS frente a sus clientes se rigen por los acuerdos celebrados con AWS, y este documento no forma parte de ningún acuerdo entre AWS y sus clientes, ni lo modifica.

Contenido

Resumen

Este documento se centra en el pilar de la seguridad del Marco de Buena Arquitectura. Ofrece asesoramiento para ayudarlo a aplicar las prácticas recomendadas y las sugerencias actuales respecto del diseño, la entrega y el mantenimiento de cargas de trabajo seguras de AWS.

Introducción

El Marco de Buena Arquitectura de AWS lo ayuda a comprender las ventajas y desventajas de las decisiones que se toman al crear cargas de trabajo en AWS. Mediante la utilización del marco, aprenderá acerca de las prácticas recomendadas de arquitectura actuales para el diseño y la operación de cargas de trabajo en la nube fiables, seguras, eficientes y rentables. Ofrece una forma de medir de manera consistente la carga de trabajo en función de las prácticas recomendadas, además de permitir identificar las áreas con posibilidad de mejora. Creemos que tener cargas de trabajo con buena arquitectura aumenta considerablemente la probabilidad de éxito empresarial.

El marco se basa en cinco pilares:

- Excelencia operativa
- Seguridad
- Fiabilidad
- Eficiencia del rendimiento
- Optimización de costos

Este documento se centra en el pilar de la seguridad. Esto lo ayudará a satisfacer los requisitos normativos y del negocio si sigue las recomendaciones actuales de AWS. Está dirigido a quienes ocupan roles tecnológicos, como los directores de tecnología (CTO), los directores de seguridad de la información (CSO/CISO), los arquitectos, los desarrolladores y los miembros de equipos operativos.

Después de leer este documento, comprenderá las recomendaciones y las estrategias actuales de AWS que conviene utilizar a la hora de diseñar una arquitectura en la nube con un enfoque de seguridad. Este documento no ofrece detalles sobre la implementación ni patrones de arquitectura, pero incluye referencias a los recursos indicados para obtener esta información. Si adopta las prácticas que se especifican en este documento, puede crear arquitecturas capaces de proteger los datos y los sistemas, controlar el acceso y responder de forma automática ante incidentes de seguridad.

Seguridad

El pilar de la seguridad describe cómo aprovechar las tecnologías de la nube para proteger los datos, los sistemas y los recursos en forma tal que pueda mejorar su posición de seguridad. Este documento ofrece asesoramiento sumamente completo sobre las prácticas recomendadas para diseñar la arquitectura de cargas de trabajo seguras en AWS.

Principios de diseño

En la nube, rigen varios principios que pueden ayudarlo a fortalecer la seguridad de la carga de trabajo:

- **Implemente una base de identidad sólida:** implemente el principio de mínimo privilegio y aplique la separación de tareas con la autorización indicada para cada interacción con los recursos de AWS. Centralice la administración de la identidad y elimine la dependencia de las credenciales estáticas y duraderas.
- **Habilite la trazabilidad:** monitoree, alerte y audite las acciones y los cambios del entorno en tiempo real. Integre la recopilación de registros y métricas con los sistemas para investigar y tomar medidas automáticamente.
- **Aplique la seguridad en todos los niveles:** implemente un enfoque de defensa sumamente completo con múltiples controles de seguridad. Aplíquelo en todos los niveles (por ejemplo: al extremo de la red, VPC, balanceo de carga, todas las instancias y servicios informáticos, sistema operativo, aplicaciones y código).
- **Automatice las prácticas recomendadas de seguridad:** los mecanismos de seguridad automatizados basados en software mejoran la capacidad para escalar con seguridad de manera más rápida y rentable. Cree arquitecturas seguras mediante la implementación de controles que se definen y administran como código en plantillas de versión controlada.
- **Proteja los datos en tránsito y en reposo:** clasifique los datos en niveles de confidencialidad y utilice mecanismos como el cifrado, la tokenización y el control de acceso, según corresponda.
- **Aleje a las personas de los datos:** utilice mecanismos y herramientas para reducir o eliminar la necesidad de acceso directo o de un procesamiento manual de datos. Esto reduce los riesgos de uso incorrecto, modificación o error humano durante la manipulación de datos confidenciales.

- **Prepárese para los incidentes de seguridad:** esté listo para los incidentes mediante una política y procesos de administración e investigación de incidentes que se ajusten a las necesidades de la organización. Ejecute simulaciones de respuesta ante incidentes y utilice herramientas con automatización para aumentar la velocidad de detección, investigación y recuperación.

Definición

La seguridad en la nube está compuesta por cinco áreas:

1. Administración de identidades y accesos
2. Detección
3. Protección de la infraestructura
4. Protección de los datos
5. Respuesta ante incidentes

La seguridad y la conformidad son una responsabilidad compartida entre AWS y usted, el cliente. El modelo compartido puedo ayudar a reducir la carga operativa. Debe examinar con cuidado los servicios que elige, ya que las responsabilidades varían en función de los servicios utilizados, la integración de aquellos servicios en el entorno de TI, y las leyes y las normas correspondientes. La naturaleza de esta responsabilidad compartida también proporciona la flexibilidad y el control que permiten la implementación.

Operación segura de la carga de trabajo

Para operar la carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de la seguridad. Tome los requisitos y los procesos que ha definido en la excelencia operativa a nivel de la organización y la carga de trabajo y aplíquelos en todas las áreas. Mantenerse al día con las recomendaciones del sector y AWS y la inteligencia de amenazas facilita la evolución del modelo de amenazas y los objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación permiten escalar las operaciones de seguridad.

Identifique y priorice riesgos mediante un modelo de amenazas: utilice un modelo de amenazas para identificar y mantener un registro actualizado de posibles amenazas. Priorice las amenazas y adapte los controles de seguridad para prevenirlas, detectarlas y responder ante ellas. Revise y mantenga esto en el contexto del panorama de seguridad en evolución.

Identifique y valide los objetivos de control: defina y valide los controles y los objetivos de control que necesita aplicar a la carga de trabajo en función de los requisitos de conformidad y los riesgos identificados en el modelo de amenazas. La validación constante de los controles y los objetivos de control facilitan la medición de la efectividad de la mitigación de riesgos.

Manténgase al día con las amenazas de seguridad: reconozca los vectores de ataque. Para ello, manténgase al día con las amenazas de seguridad más recientes a fin de facilitar la definición y la implementación de los controles apropiados.

Manténgase al día con las recomendaciones de seguridad: manténgase al día con las recomendaciones de AWS y las del sector en materia de seguridad a fin de impulsar el desarrollo de la posición de seguridad de la carga de trabajo.

Evalúe e implemente nuevos servicios y características de seguridad con frecuencia: evalúe e implemente los servicios y las características de seguridad de AWS y los socios de APN que permitan el desarrollo de la posición de seguridad de la carga de trabajo.

Automatice las pruebas y la validación de los controles de seguridad en las canalizaciones: establezca plantillas y puntos de referencia seguros para los mecanismos de seguridad que se prueban y validan como parte de la creación, las canalizaciones y los procesos. Utilice herramientas y la automatización para probar y validar todos los controles de seguridad de forma continua. Por ejemplo, analice elementos, como las imágenes de máquinas y la infraestructura, como plantillas de código para detectar vulnerabilidades de seguridad, irregularidades y desviaciones con respecto al punto de referencia establecido en cada etapa.

Reducir la cantidad de errores de configuración introducidos en un entorno de producción es fundamental. Es preferible que haya más controles de calidad y medidas para reducir los errores durante el proceso de creación. Diseñe canalizaciones de integración e implementación continuas (CI/CD) para realizar pruebas que detecten problemas de seguridad siempre que sea posible. Las canalizaciones de CI/CD ofrecen la posibilidad de mejorar la seguridad en todas las etapas de creación y entrega. Las herramientas de seguridad de CI/CD también se deben mantener actualizadas para mitigar las amenazas en constante desarrollo.

Recursos

Consulte los siguientes recursos para obtener más información acerca de la operación segura de la carga de trabajo.

Videos

- 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

Documentación

- Información general acerca de los procesos de seguridad
- Boletines de seguridad
- Blog de seguridad
- Novedades de AWS
- Directivas de auditoría de seguridad de AWS
- Configurar una canalización de CI/CD en AWS

Separación y administración de cuentas de AWS

Recomendamos que organice las cargas de trabajo en cuentas individuales y agrupe cuentas según la función, los requisitos de conformidad o un conjunto común de controles en lugar de imitar la estructura de informes de su empresa. En AWS, las cuentas son un contenedor de confianza cero con límites estrictos para los recursos. Por ejemplo, es absolutamente recomendable la separación a nivel de cuenta para aislar las cargas de trabajo de producción de las cargas de trabajo de desarrollo y prueba.

Separe las cargas de trabajo mediante el uso de cuentas: comience teniendo en cuenta la seguridad y la infraestructura para permitir que su organización establezca medidas de seguridad conforme crezcan las cargas de trabajo. Este enfoque establece límites y controles entre las cargas de trabajo. Se recomienda enfáticamente la separación a nivel de cuenta para aislar los entornos de producción de los entornos de desarrollo y de prueba; o bien, establecer un límite lógico sólido entre las cargas de trabajo que procesan datos de diferentes niveles de confidencialidad, de acuerdo con los requisitos de conformidad externos (como PCI-DSS o HIPAA), y las cargas de trabajo que no lo hacen.

Proteja las cuentas de AWS: existen varios aspectos para proteger las cuentas de AWS, incluida la seguridad, pero no el uso, del usuario raíz y el mantenimiento actualizado de la información de contacto. Puede utilizar AWS Organizations para administrar y controlar sus cuentas de forma centralizada a medida que aumenta y escala las cargas de trabajo. AWS Organizations lo ayuda a administrar las cuentas, establecer los controles y configurar los servicios en todas sus cuentas.

Administre las cuentas de forma centralizada: AWS Organizations automatiza la creación y la administración de las cuentas de AWS y el control de estas cuentas después de su creación. Cuando se crea una cuenta a través de AWS Organizations, es importante tener en cuenta la dirección de email que se utiliza, ya que esta será el usuario raíz que permitirá restablecer la contraseña. Organizations le permite agrupar las cuentas en unidades organizativas (OU) que pueden representar diferentes entornos en función de los requisitos y el objetivo de la carga de trabajo.

Establezca controles de forma centralizada: para controlar lo que pueden hacer sus cuentas de AWS, solo permita servicios, regiones y acciones de servicios específicos en los niveles apropiados. AWS Organizations le permite utilizar políticas de control de servicios (SCP) para aplicar medidas de seguridad de los permisos a nivel de organización, de unidad organizativa o de cuenta, que se aplican a todos los usuarios y roles de AWS Identity and Access Management (IAM). Por ejemplo, puede aplicar una SCP que impida que los usuarios lancen recursos en las regiones que no ha permitido de forma explícita. AWS Control Tower ofrece una forma simplificada de configurar y controlar varias cuentas. Automatiza la configuración de las cuentas en su organización de AWS y el aprovisionamiento, aplica medidas de seguridad (que incluyen la prevención y la detección) y le ofrece un panel para la visibilidad.

Configure servicios y recursos de forma centralizada: AWS Organizations lo ayuda a configurar los servicios de AWS que se aplican a todas sus cuentas. Por ejemplo, puede configurar el registro centralizado de todas las acciones que se realizan en su organización con AWS CloudTrail y evitar que las cuentas miembro deshabiliten el registro. También puede agregar datos de forma centralizada para las reglas que ha definido con AWS Config, lo que le permite auditar la conformidad de las cargas de trabajo y reaccionar rápidamente a los cambios. AWS CloudFormation StackSets le permite administrar de forma centralizada las pilas de AWS CloudFormation en todas las cuentas y las unidades organizativas de su organización. Esto le permite aprovisionar una cuenta nueva de forma automática para cumplir con sus requisitos de seguridad.

Recursos

Consulte los siguientes recursos a fin de obtener más información acerca de las recomendaciones de AWS para implementar y administrar múltiples cuentas de AWS.

Videos

- 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

Documentación

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

Práctica

- Laboratorio: AWS Account and Root User

Administración de identidades y accesos

Para utilizar los servicios de AWS, debe otorgar a los usuarios y las aplicaciones acceso a los recursos en sus cuentas de AWS. A medida que ejecuta más cargas de trabajo en AWS, necesita una administración de la identidad sólida y permisos para garantizar que las personas apropiadas tengan acceso a los recursos apropiados en las condiciones apropiadas. AWS ofrece una amplia selección de capacidades para ayudarlo a administrar sus identidades de humanos y de máquinas y sus permisos. Las prácticas recomendadas para estas capacidades se pueden dividen en dos áreas principales:

- Administración de la identidad
- Administración de permisos

Administración de la identidad

Existen dos tipos de identidades que necesitará administrar cuando aborde las cargas de trabajo operativas de AWS seguras.

Identidades de humanos: los administradores, los desarrolladores, los operadores y los consumidores de sus aplicaciones necesitan una identidad para obtener acceso a los entornos y a las aplicaciones de AWS. Pueden ser miembros de su organización o usuarios externos con los que colabora, que interactúan con sus recursos de AWS mediante un navegador web, una aplicación cliente, una aplicación móvil o herramientas interactivas de línea de comandos.

Identidades de máquinas: las aplicaciones de las cargas de trabajo, las herramientas operativas y los componentes requieren una identidad para realizar solicitudes a los servicios de AWS, como, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su entorno de AWS, como las instancias de Amazon EC2 o las funciones de AWS Lambda. También puede administrar las identidades de máquinas para los usuarios externos que necesiten acceso. Además, puede tener máquinas fuera de AWS que necesiten acceso a su entorno de AWS.

Uso de un proveedor centralizado de identidad

Para las identidades del personal, utilice un proveedor de identidad que le permita administrar las identidades en un lugar centralizado. Esto facilita la administración del acceso en múltiples aplicaciones y servicios, ya que está creando, administrando y revocando el acceso desde una única ubicación. Por ejemplo, si alguien abandona su organización, puede revocar el acceso a todas las aplicaciones y los servicios (incluido AWS) desde una ubicación. Esto elimina la necesidad de tener múltiples credenciales y brinda la oportunidad de integrarse a los procesos de RR. HH. existentes.

En cuanto a la federación con cuentas individuales de AWS, puede usar identidades centralizadas para AWS con un proveedor basado en SAML 2.0 con AWS IAM. Puede usar cualquier proveedor,ya sea alojado por usted en AWS, externo a AWS o suministrado por la red de socios de AWS (APN), que sea compatible con el protocolo de SAML 2.0. Puede usar la federación entre su cuenta de AWS y el proveedor elegido para conceder a un usuario o una aplicación acceso a fin de llamar a las operaciones de la API de AWS con una aserción SAML y obtener credenciales de seguridad temporales. También se admite el inicio de sesión único basado en la Web, lo que permite a los usuarios iniciar sesión en la consola de administración de AWS desde su portal de inicio de sesión.

En el caso de la federación para varias cuentas en su organización de AWS, puede configurar su origen de identidad en AWS Single Sign-On (AWS SSO) y especificar dónde se almacenan sus usuarios y sus grupos. Una vez que esté configurado, su proveedor de identidad es su fuente de verdad, y la información puede sincronizarse con el protocolo System for Cross-domain Identity Management (SCIM) v2.0. Luego, puede buscar usuarios o grupos, y concederles acceso de inicio de sesión único a las cuentas de AWS, a las aplicaciones en la nube o a ambas.

AWS SSO se integra a AWS Organizations, lo que le permite configurar su proveedor de identidad una vez y, luego, conceder acceso a las cuentas existentes y nuevas administradas en su organización. AWS SSO le proporciona un almacén predeterminado, que puede usar para administrar sus usuarios y sus grupos. Si elige usar el almacén de AWS SSO, cree sus usuarios y sus grupos y asigne el nivel de acceso a las aplicaciones y las cuentas de AWS, y tenga en cuenta la práctica recomendada de privilegio mínimo. De manera alternativa, puede elegir Conectarse a su proveedor de identidad externo usando SAML 2.0 o Conectarse a su Microsoft AD Directory usando AWS Directory Service. Una vez que esté configurado, puede iniciar sesión en la consola de administración de AWS, la interfaz de línea de comandos o la aplicación móvil de AWS, mediante la autenticación a través de su proveedor de identidad central.

Para administrar los usuarios finales o los consumidores de sus cargas de trabajo, como una aplicación móvil, puede usar Amazon Cognito. Proporciona autenticación, autorización y administración de usuarios para las aplicaciones web y móviles. Sus usuarios pueden iniciar sesión directamente con un nombre de usuario y una contraseña, o a través de un tercero como Amazon, Apple, Facebook o Google.

Uso de los grupos y los atributos de usuarios

A medida que aumenta la cantidad de usuarios que usted administra, necesitará determinar maneras de organizarlos para poder administrarlos a escala. Ubique a los usuarios con requisitos de seguridad comunes en grupos definidos según su proveedor de identidad e implemente mecanismos para garantizar que los atributos de los usuarios que se puedan utilizar para controlar el acceso (por ejemplo, departamento o ubicación) sean correctos y estén actualizados. Utilice estos grupos y atributos para controlar el acceso, en lugar de los usuarios

individuales. Esto le permite administrar el acceso de manera centralizada al cambiar la pertenencia a un grupo de usuarios o los atributos solo una vez con un conjunto de permisos, en lugar de actualizar varias políticas individuales cuando necesita cambiar el acceso de un usuario. Puede usar AWS SSO para administrar grupos de usuarios y atributos. AWS SSO admite la mayoría de los atributos que se suelen utilizar, sin importar si se ingresan de forma manual durante la creación del usuario o si se aprovisionan con un motor de sincronización de manera automática, tal como se define en la especificación de System for Cross-Domain Identity Management (SCIM).

Uso de mecanismos de inicio de sesión seguros

Aplique contraseñas de longitud mínima e instruya a sus usuarios para que eviten elegir contraseñas comunes o que ya utilizaron. Aplique la autenticación multifactor (MFA) con mecanismos de software o hardware para ofrecer una capa adicional de verificación. Por ejemplo, cuando use AWS SSO como origen de identidad, configure el parámetro "context-aware" o "always-on" para MFA y permita a los usuarios inscribir sus propios dispositivos de MFA para acelerar la adopción. Cuando use un proveedor de identidad (IdP) externo, configure su IdP para MFA.

Uso de credenciales temporales

Solicite a las identidades que adquieran credenciales temporales de manera dinámica. En cuanto a las identidades del personal, utilice AWS SSO o la federación con IAM para acceder a las cuentas de AWS. Con respecto a las identidades de máquinas, como las instancias EC2 o las funciones de Lambda, solicite el uso de roles de IAM en lugar de usuarios de IAM con claves de acceso a largo plazo.

Para las identidades de humanos que utilizan la consola de administración de AWS, solicite a los usuarios que adquieran credenciales temporales y se federen en AWS. Puede hacer esto usando el portal de usuario de AWS SSO o configurando la federación con IAM. En el caso de los usuarios que requieren acceso a la CLI, asegúrese de que usen AWS CLI v2, que admite la integración directa a AWS Single Sign-On (AWS SSO). Los usuarios pueden crear perfiles de la CLI que están vinculados a las cuentas y los roles de AWS SSO. La CLI recupera automáticamente las credenciales de AWS desde AWS SSO y las actualiza en su nombre. De esta forma, no hay necesidad de copiar y pegar las credenciales temporales de AWS desde la consola de AWS SSO. En el caso de los SDK, los usuarios deben confiar en que AWS STS asuma los roles para recibir credenciales temporales. En determinados casos, es posible que las credenciales temporales no sean prácticas. Debe tener en cuenta los riesgos de almacenar claves de acceso, rotarlas con frecuencia y requerir MFA como condición cuando sea posible.

En los casos en que deba conceder acceso a sus recursos de AWS a los consumidores, use los grupos de identidades de Amazon Cognito y asígneles un conjunto de credenciales temporales con privilegio limitado para acceder a sus recursos de AWS. Los permisos de cada usuario son

controlados a través de los roles de IAM que usted crea. Puede definir reglas para elegir el rol de cada usuario en función de las reclamaciones del token de ID del usuario. Puede definir un rol predeterminado para los usuarios autenticados. También puede definir un rol de IAM independiente con permisos limitados para los usuarios invitados que no están autenticados.

En el caso de las identidades de máquinas, debe confiar en los roles de IAM para conceder acceso a AWS. En cuanto a las instancias EC2, puede usar los roles para Amazon EC2. Puede asociar un rol de IAM a su instancia EC2 para permitir que las aplicaciones que se ejecutan en Amazon EC2 usen credenciales de seguridad temporales que AWS crea, distribuye y rota de manera automática. Con respecto al acceso a las instancias EC2 con claves o contraseñas, AWS Systems Manager es una manera más segura de obtener acceso a sus instancias y administrarlas usando un agente instalado previamente sin el secreto almacenado. Además, otros servicios de AWS, como AWS Lambda, le permiten configurar un rol de servicio de IAM para conceder permisos de servicio con el fin de realizar acciones de AWS usando credenciales temporales.

Auditoría y rotación periódica de las credenciales

La validación periódica, preferiblemente mediante una herramienta automatizada, es necesaria para verificar que se apliquen los controles correctos. En el caso de identidades de humanos, debe requerir a los usuarios cambiar periódicamente sus contraseñas y retirar las claves de acceso en favor de las credenciales temporales. También recomendamos que monitoree continuamente los ajustes de MFA en su proveedor de identidades. Puede configurar las reglas de AWS Config para monitorear estos ajustes. En el caso de las identidades de máquinas, debe confiar en las credenciales temporales que usan roles de IAM. En situaciones en las que esto no es posible, es necesario realizar auditorías frecuentes y rotar las claves de acceso.

Almacenamiento y uso seguro de los secretos

Para las credenciales que no están relacionadas con IAM, como, por ejemplo, el inicio de sesión de una base de datos, utilice un servicio diseñado para administrar los secretos, como AWS Secrets Manager. AWS Secrets Manager facilita la administración, la rotación y el almacenamiento seguro de secretos cifrados que usan servicios admitidos. Las llamadas para obtener acceso a los secretos se registran en CloudTrail con fines de auditoría. Los permisos de IAM pueden conceder acceso con privilegio mínimo a ellos.

Recursos

Consulte los siguientes recursos para obtener más información sobre las prácticas recomendadas de AWS para la protección de las credenciales de AWS.

Videos

- 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

Documentación

- El usuario raíz de la cuenta de AWS
- Credenciales de usuario de la cuenta raíz de AWS frente a credenciales de usuario de IAM
- Las prácticas recomendadas de IAM
- Configuración de una política de contraseñas de la cuenta para los usuarios de IAM
- Introducción a AWS Secrets Manager
- Uso de perfiles de instancia
- Credenciales de seguridad temporales
- Federación y proveedores de identidades

Administración de permisos

Administre los permisos para controlar el acceso a las identidades de las personas y de las máquinas que requieran acceso a AWS y a su carga de trabajo. Los permisos controlan a qué se tiene acceso, quién puede acceder y bajo qué condiciones lo hace. Establezca permisos para identidades específicas de máquinas y de humanos con el fin de conceder acceso a acciones de servicio específicas en recursos determinados. Además, especifique condiciones que deben ser verdaderas para que se conceda el acceso. Por ejemplo, puede permitir a los desarrolladores crear nuevas funciones de Lambda, pero solo en una región específica. Cuando administre sus entornos de AWS a escala, cumpla con las siguientes prácticas recomendadas para garantizar que las identidades solo tengan el acceso que necesitan y nada más.

Definición de las medidas de seguridad de los permisos para su organización

A medida que aumente y administre cargas de trabajo adicionales en AWS, debe separar estas cargas de trabajo usando cuentas y administrar estas cuentas con AWS Organizations. Recomendamos que establezca medidas de seguridad de permiso comunes que limiten el acceso a todas las identidades de su organización. Por ejemplo, puede limitar el acceso a regiones de AWS específicas o evitar que sus equipo borre recursos comunes, tales como los roles de IAM utilizados por su equipo de seguridad central. Puede comenzar implementando

un ejemplo de políticas de control de servicios, como evitar que los usuarios desactiven servicios claves.

Puede usar AWS Organizations para agrupar cuentas y establecer controles comunes en cada grupo de cuentas. Para establecer estos controles comunes, puede usar servicios integrados a AWS Organizations. Específicamente, puede usar políticas de control de servicios (SCP) para restringir el acceso a un grupo de cuentas. Las SCP usan el lenguaje de políticas de IAM y le permiten establecer controles con los que cumplen todos los elementos principales de IAM (usuarios y roles). Puede establecer restricciones de acceso a acciones y recursos de servicio específicos en función de condiciones específicas para satisfacer las necesidades de control de su organización. Si es necesario, puede definir excepciones para sus medidas de seguridad. Por ejemplo, puede restringir acciones de servicio para todas las entidades de IAM en la cuenta, salvo para un rol de administrador específico.

Autorización de acceso con privilegios mínimos

El establecimiento de un principio de mínimo privilegio asegura que a las identidades solo se les permita realizar el conjunto mínimo de funciones necesarias para cumplir una tarea específica, al tiempo que se equilibran la facilidad de uso y la eficiencia. Operar bajo este principio limita el acceso no deseado y ayuda a asegurar que usted decida quién tiene acceso a cada recurso. En AWS, las identidades no tienen permisos predeterminados con la excepción del usuario raíz, que solo se debe usar para tareas específicas nuevas.

Usa políticas para conceder explícitamente permisos asociados a IAM o entidades de recursos, como un rol de IAM usado por identidades federadas o máquinas o por recursos (por ejemplo, buckets de S3). Cuando crea y asocia una política, puede especificar las acciones, los recursos y las condiciones de servicio que deben ser verdaderos para que AWS permita el acceso. AWS admite una serie de condiciones para ayudarlo a limitar el acceso. Por ejemplo, si se utiliza la clave de condición PrincipalOrgID, se verifica el identificador de AWS Organizations para que se pueda conceder acceso dentro de su organización de AWS. También puede controlar las solicitudes que realizan los servicios de AWS en su nombre, como AWS CloudFormation que crea una función de AWS Lambda, mediante el uso de la clave de condición CalledVia. Esto le permite establecer permisos detallados para las identidades de humanos y de máquinas en AWS.

AWS también tiene capacidades que le permiten escalar su administración de permisos y cumplir con el privilegio mínimo.

Límites de permisos: puede utilizar límites de permisos para establecer la cantidad máxima de permisos que puede fijar un administrador. Esto le permite delegar la capacidad de crear y administrar permisos a los desarrolladores, como la creación de un rol de IAM, pero también limitar los permisos que pueden conceder, de manera que no puedan escalar su privilegio usando lo que crearon.

Control de acceso basado en atributos (ABAC): AWS le permite conceder permisos basados en atributos. En AWS, de denominan "etiquetas". Las etiquetas se pueden asociar a los elementos principales de IAM (usuarios o roles) y a los recursos de AWS. Con las políticas de IAM, los administradores pueden crear una política reutilizable que aplique los permisos basados en los atributos de los elementos principales de IAM. Por ejemplo, como administrador, usted puede usar una política de IAM única que conceda a los desarrolladores de su organización acceso a los recursos de AWS que coincidan con las etiquetas del proyecto de los desarrolladores. A medida que el equipo de desarrolladores agrega recursos a los proyectos, los permisos se aplican automáticamente en función de los atributos. Como resultado, no se requiere una actualización de la política para cada nuevo recurso.

Análisis del acceso público y el acceso entre cuentas

En AWS, puede conceder acceso a los recursos en otra cuenta. Puede conceder acceso directo entre cuentas usando políticas asociadas a los recursos (por ejemplo, políticas de buckets de S3) o permitiendo que una identidad asuma un rol de IAM en otra cuenta. Cuando use políticas de recursos, debe asegurarse de conceder acceso a las identidades en su organización y de que tenga la intención de hacer público un recurso. Cuando haga público un recurso, debe hacerlo con moderación, ya que esta acción permite que cualquier persona tenga acceso al recurso. El analizador de acceso IAM usa métodos matemáticos (es decir, seguridad comprobable) para identificar todas las rutas de acceso a un recurso desde afuera de su cuenta. Revisa las políticas de recursos de manera continua e informa los resultados de acceso público y de acceso entre cuentas para que le resulte más fácil analizar el acceso potencialmente amplio.

Uso compartido seguro de los recursos

A medida que administra cargas de trabajo usando cuentas independientes, habrá casos en los que necesitará compartir los recursos entre esas cuentas. Recomendamos que comparta recursos mediante AWS Resource Access Manager (AWS RAM). Este servicio le permite compartir recursos de AWS dentro de sus unidades organizativas y su organización de AWS de manera sencilla y segura. Con AWS RAM, el acceso a los recursos compartidos se otorga o revoca de manera automática, ya que las cuentas se mueven dentro o fuera de la organización o de la unidad organizativa con la cual se comparten. Esto lo ayuda a asegurarse de que los recursos solo se compartan con las cuentas que desea.

Reducción de la cantidad permisos de manera continua

A veces, cuando los equipos y los proyectos están en sus comienzos, es probable que se opte por otorgar acceso amplio con el fin de inspirar innovación y agilidad. Recomendamos que evalúe el acceso de manera continua y que restrinja el acceso a solo los permisos necesarios para así lograr privilegios mínimos. AWS brinda capacidades de análisis del acceso que lo

ayudan a identificar el acceso no utilizado. Para ayudarlo a identificar usuarios y roles no utilizados, AWS analiza la actividad de acceso y proporciona información sobre el último uso del rol y la clave de acceso. Puede utilizar la marca temporal del último acceso a fin de identificar usuarios y roles no utilizados para luego eliminarlos. Además, puede revisar la información sobre la última vez que se accedió al servicio y la acción con el fin de identificar y ajustar los permisos para usuarios y roles específicos. Por ejemplo, puede utilizar la información sobre la última vez en que se obtuvo acceso con el fin de identificar las acciones de S3 específicas que el rol de la aplicación necesita y así limitar el acceso a ellas solamente. Estas características están disponibles en la consola y mediante programación para que pueda incorporarlas en los flujos de trabajo de la infraestructura y las herramientas automatizadas.

Establecimiento de un proceso de acceso de emergencia

Debe contar con un proceso que permita el acceso de emergencia a la carga de trabajo, en particular a sus cuentas de AWS, ante el insólito caso de que se produzca un problema de canalización o proceso automatizado. Este proceso podría incluir una combinación de distintas capacidades, por ejemplo, un rol entre cuentas de AWS de emergencia para el acceso o un proceso específico que los administradores deberían seguir con el fin de validar y aprobar una solicitud de emergencia.

Recursos

Consulte los siguientes recursos a fin de obtener más información acerca de las prácticas recomendadas de AWS actuales para la autorización detallada.

Videos

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

Documentación

- Conceder privilegios mínimos
- Administración de políticas
- Delegación de permisos para la administración de usuarios, grupos y credenciales de IAM
- Analizador de acceso de IAM
- Eliminar credenciales innecesarias
- Asumir un rol en la CLI con MFA
- Límites de permisos
- Control de acceso basado en atributos (ABAC)

Práctica

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

Detección

La detección le permite identificar una posible configuración errónea de seguridad, una amenaza o un comportamiento inesperado. Es una parte esencial del ciclo de vida de la seguridad y se puede utilizar para admitir un proceso de calidad o una obligación legal o de conformidad, además de para identificar amenazas e iniciativas de respuesta. Existen diferentes tipos de mecanismos de detección. Por ejemplo, los registros de la carga de trabajo se pueden analizar en busca de vulnerabilidades que se estén utilizando. Debe revisar los mecanismos de detección relacionados con la carga de trabajo de manera regular para asegurarse de que está cumpliendo los requisitos y las políticas tanto internos como externos. Las alertas y las notificaciones automatizadas se deben basar en condiciones definidas para permitir que los equipos o las herramientas investiguen. Estos mecanismos son factores reactivos importantes que pueden ayudar a la organización a identificar y comprender el alcance de la actividad anómala.

En AWS, existen varios enfoques que puede utilizar al momento de abordar los mecanismos de detección. Las siguientes secciones describen cómo utilizar esos enfoques:

- Configuración
- Investigación

Configuración

Configure el registro de los servicios y las aplicaciones: una práctica fundamental consiste en establecer un conjunto de mecanismos de detección a nivel de cuenta. Este conjunto base de mecanismos está diseñado para registrar y detectar una amplia gama de acciones en todos los recursos de su cuenta. Estos mecanismos le permiten construir una capacidad de detección integral con opciones que incluyen la corrección automatizada y las integraciones de socios para agregar funcionalidad.

En AWS, los servicios en este conjunto base incluyen los siguientes:

- AWS CloudTrail proporciona el historial de eventos de la actividad de su cuenta de AWS, incluidas las acciones realizadas a través de la consola de administración de AWS, los SDK de AWS, las herramientas de la línea de comandos y otros servicios de AWS.
- AWS Config monitorea y registra las configuraciones de los recursos de AWS y le permite automatizar la evaluación y la corrección en función de las configuraciones deseadas.
- Amazon GuardDuty es un servicio de detección de amenazas que monitorea continuamente a fin de encontrar actividad maliciosa y comportamiento no autorizado a fin de proteger las cuentas y las cargas de trabajo de AWS.

- AWS Security Hub proporciona un solo lugar donde se agrupan, organizan y priorizan sus alertas de seguridad o hallazgos de múltiples servicios de AWS y productos opcionales de terceros. Esto permite brindarle una visión integral de las alertas de seguridad y el estado de conformidad.

Al crear sobre el nivel de cuenta, muchos servicios fundamentales de AWS, como Amazon Virtual Private Cloud (VPC), proporcionan características de registro a nivel de servicio. Los registros de flujo de VPC le permiten captar información sobre el tráfico IP que entra y sale de las interfaces de redes, lo que puede proporcionar información valiosa acerca del historial de conectividad, así como desencadenar acciones automatizadas en función del comportamiento anómalo.

Para el registro basado en aplicaciones e instancias EC2 que no se genera en servicios de AWS, los registros se pueden almacenar y analizar mediante Amazon CloudWatch Logs. Un agente recopila los registros del sistema operativo y las aplicaciones que se están ejecutando y los almacena automáticamente. Una vez que los registros estén disponibles en CloudWatch Logs, puede procesarlos en tiempo real o realizar un análisis con Insights.

La capacidad de extraer información significativa de los grandes volúmenes de datos de registros y eventos generados por arquitecturas complejas es tan importante como recopilar y agrupar registros. Consulte la sección *Monitoreo* del documento técnico El pilar de fiabilidad para obtener más información. Los registros en sí mismos pueden contener datos que se consideran confidenciales, ya sea cuando los datos de la aplicación aparecen erróneamente en los archivos de registro que el agente de CloudWatch Logs captura o cuando el registro entre regiones se configura para agrupar registros y existen consideraciones legislativas sobre el envío de ciertos tipos de información a través de fronteras.

Un enfoque consiste en utilizar las funciones de Lambda activadas en los eventos cuando se entregan los registros, a fin de filtrar y redactar los datos de registro antes de enviarlos a una ubicación central de registro, como un bucket de S3. Los registros sin modificaciones se pueden retener en un bucket local hasta que haya transcurrido un “periodo razonable” (según determine la legislación y el equipo jurídico), después del cual una regla de ciclo de vida de S3 tiene permitido eliminarlos de manera automática. Adicionalmente, los registros se pueden proteger en Amazon S3 a través del bloqueo de objetos de S3, por el cual se pueden almacenar objetos mediante un modelo de escritura única y lectura múltiple (WORM).

Analice los registros, los hallazgos y las métricas de manera centralizada: los equipos de operaciones de seguridad recurren a la recopilación de registros y al uso de herramientas de búsqueda para descubrir posibles eventos de interés, que podrían indicar actividad no autorizada o cambio no voluntario. Sin embargo, el simple análisis de los datos recopilados y el procesamiento manual de la información no es suficiente para seguir el ritmo del volumen de información que fluye de las arquitecturas complejas. El análisis y la elaboración de informes por sí solos no facilitan la asignación de los recursos adecuados para gestionar un evento de manera oportuna.

Una práctica recomendada para crear un equipo de operaciones de seguridad maduro implica integrar profundamente el flujo de los eventos y los hallazgos de seguridad en un sistema de notificaciones y flujo de trabajo, como un sistema de emisión de tickets, un sistema de errores y problemas, u otro sistema de administración de información y eventos de seguridad (SIEM). Esto saca el flujo de trabajo de los informes de email y estáticos, y permite dirigir, escalar y administrar eventos o hallazgos. Muchas organizaciones también integran alertas de seguridad en sus plataformas de chat o colaboración, y de productividad de los desarrolladores. Para las organizaciones que comienzan a implementar la automatización, un sistema de emisión de tickets de baja latencia y basado en la API ofrece una flexibilidad significativa a la hora de planificar "qué hay que automatizar primero".

Esta práctica recomendada no solo se aplica a los eventos de seguridad generados a partir de los mensajes de registro que describen la actividad de los usuarios o los eventos de la red, sino también a los cambios detectados en la propia infraestructura. La capacidad de detectar el cambio, de determinar si un cambio es apropiado y de, luego, dirigir esa información al flujo de trabajo de corrección indicado es esencial a la hora de mantener y validar una arquitectura segura, en un contexto de cambios en el que la naturaleza de no ser deseados es lo suficientemente sutil como para que su ejecución no se pueda evitar en este momento con una combinación de configuración de Organizations e IAM.

GuardDuty y Security Hub proporcionan mecanismos para agrupar, desduplicar y analizar los registros que también están disponibles a través de otros servicios de AWS. Específicamente, GuardDuty incorpora, agrupa y analiza información del servicio de DNS de la VPC e información que de otra manera se puede ver a través de CloudTrail y los registros de flujo de la VPC. Security Hub puede incorporar, agrupar y analizar los resultados de GuardDuty, AWS Config, Amazon Inspector, Macie, AWS Firewall Manager y un número significativo de productos de seguridad de terceros que están disponibles en AWS Marketplace, y, si se compila en consecuencia, también su propio código. Tanto GuardDuty como Security Hub tienen un modelo de miembro maestro que puede agrupar los hallazgos y la información de múltiples cuentas. Además, con frecuencia, Security Hub suele ser la herramienta de preferencia de los clientes que tienen un SIEM en las instalaciones como un registro del lado de AWS y un preprocesador y agregador de alertas desde los cuales pueden luego incorporar Amazon EventBridge a través de un procesador y reenviador basados en Lambda.

Recursos

Consulte los siguientes recursos a fin de obtener más información acerca de las recomendaciones actuales de AWS para la captura y el análisis de registros.

Videos

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

Documentación

- Configuración de Amazon GuardDuty
- AWS Security Hub
- Introducción a Amazon CloudWatch Logs
- Amazon EventBridge
- Configuración de Athena para el análisis de los registros de CloudTrail
- Amazon CloudWatch
- AWS Config
- Creación de un registro de seguimiento en CloudTrail
- Centralize logging solution

Práctica

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

Investigación

Implemente eventos de seguridad que se puedan procesar: por cada mecanismo de detección que tenga, también debería tener un proceso en forma de un manual de procedimientos o de un manual de identificación de problemas, para investigar. Por ejemplo, cuando habilita Amazon GuardDuty, este genera diferentes hallazgos. Debe tener una entrada en el manual de procedimientos por cada tipo de hallazgo. Por ejemplo, si se descubre un troyano, el manual de procedimientos cuenta con instrucciones sencillas que indican a alguien que lleve a cabo la investigación y la corrección.

Automatice respuestas ante eventos: en AWS, la investigación de eventos de interés e información acerca de cambios potencialmente inesperados en un flujo de trabajo automatizado se puede lograr con Amazon EventBridge. Este servicio proporciona un motor de reglas escalable diseñado para gestionar los formatos de eventos nativos de AWS (como los eventos de CloudTrail) y los eventos personalizados que se pueden generar desde la aplicación. Amazon EventBridge también permite dirigir los eventos a un sistema de flujo de trabajo para aquellos que crean sistemas de respuesta ante incidentes (Step Functions) o dirigirlos a una cuenta de seguridad central, así como a un bucket que permita un análisis más detallado.

También se puede detectar el cambio y dirigir esta información al flujo de trabajo adecuado por medio de las reglas de AWS Config. AWS Config detecta cambios en los servicios

abarcados (aunque con mayor latencia que Amazon EventBridge) y genera eventos que pueden analizarse mediante las reglas de AWS Config para la restauración, la aplicación de políticas de conformidad y el envío de información a los sistemas, como las plataformas de administración de cambios y los sistemas operativos de emisión de tickets. Además de escribir sus propias funciones de Lambda para responder a los eventos de AWS Config, también puede aprovechar el Kit de desarrollo de reglas de AWS Config y una biblioteca de código abierto de reglas de AWS Config.

Recursos

Consulte los siguientes recursos a fin de obtener más información acerca de las prácticas recomendadas actuales de AWS para la integración de controles de auditoría en las notificaciones y el flujo de trabajo.

Videos

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

Documentación

- Amazon Detective
- Amazon EventBridge
- Reglas de AWS Config
- AWS Config Rules Repository (open source)
- AWS Config Rules Development Kit

Práctica

- Solución: Observaciones en tiempo real sobre la actividad de la cuenta de AWS
- Solución: Centralized Logging

Protección de la infraestructura

La protección de la infraestructura incluye metodologías de control, como la defensa en profundidad, que son necesarias para cumplir las prácticas recomendadas y las obligaciones organizacionales o normativas. La aplicación de estas metodologías es fundamental para el éxito de las operaciones en curso en la nube.

La protección de la infraestructura es una pieza clave de cualquier programa de seguridad de la información. Garantiza que los sistemas y los servicios de la carga de trabajo estén protegidos contra el acceso no intencionado y no autorizado, y contra posibles vulnerabilidades. Por ejemplo, se definirán los límites de confianza (como los límites de la red y las cuentas), la configuración y el mantenimiento de la seguridad del sistema (como el refuerzo, la minimización y la aplicación de parches), la autenticación y las autorizaciones del sistema operativo (como los usuarios, las claves y los niveles de acceso), y otros puntos adecuados para la aplicación de políticas (como los firewall de las aplicaciones web o las gateway de la API).

En AWS, existen varios enfoques para la protección de la infraestructura. Las siguientes secciones describen cómo utilizar esos enfoques:

- Protección de redes
- Protección de recursos informáticos

Protección de redes

La planificación y la administración cuidadosas del diseño de la red constituye la base de cómo se proporciona aislamiento y se establecen límites para los recursos de la carga de trabajo. Debido a que muchos recursos de la carga de trabajo operan en una VPC y heredan las propiedades de seguridad, es esencial que el diseño se admita en los mecanismos de inspección y protección respaldados por la automatización. De la misma manera, para las cargas de trabajo que operan fuera de una VPC con servicios exclusivamente de borde o sin servidor, las prácticas recomendadas se aplican según un enfoque más simple. Consulte el Enfoque de aplicaciones sin servidor del Marco de Buena Arquitectura de AWS para obtener orientación especifica acerca de la seguridad sin servidor.

Cree capas de red: los componentes, como las instancias EC2, los clústeres de bases de datos de RDS y las funciones de Lambda, que comparten requisitos de accesibilidad pueden segmentarse en capas formadas por subredes. Por ejemplo, un grupo de bases de datos de RDS en una VPC sin necesidad de contar con acceso a Internet debería colocarse en subredes sin ruta hacia o desde Internet. Este enfoque por capas para los controles mitiga el impacto de una mala configuración con una sola capa, la cual podría permitir un acceso no deseado. En el caso de AWS Lambda, se pueden ejecutar las funciones en la VPC a fin de aprovechar los controles basados en la VPC.

Para la conectividad de la red que puede incluir miles de VPC, cuentas de AWS y redes en las instalaciones, debe utilizar AWS Transit Gateway. Actúa como un centro que controla la forma en que se dirige el tráfico entre todas las redes conectadas, las cuales actúan como radios de una rueda. El tráfico entre Amazon VPC y AWS Transit Gateway permanece en la red privada de AWS, lo que reduce los vectores de amenazas externas, como los ataques de denegación de servicio distribuido (DDoS) y los ataques comunes, como la inyección SQL, el scripting en sitios cruzados, la falsificación de solicitudes en sitios cruzados o el abuso de código de

autenticación roto. La interconexión entre regiones de AWS Transit Gateway también cifra el tráfico entre regiones sin un punto único de error o cuello de botella de ancho de banda.

Controle el tráfico en todas las capas: al diseñar la topología de su red, debe examinar los requisitos de conectividad de cada componente. Por ejemplo, analice si un componente requiere accesibilidad a Internet (de entrada y salida), conectividad a las VPC, servicios de borde y centros de datos externos.

Una VPC le permite definir la topología de la red que se extiende a lo largo de una región de AWS con un rango de direcciones IPv4 privadas que usted establece, o un rango de direcciones IPv6 que AWS selecciona. Debe aplicar múltiples controles con un enfoque de defensa en profundidad tanto para el tráfico de entrada como para el de salida, incluido el uso de grupos de seguridad (firewall de inspección con estado), listas de control de acceso (ACL) de red, subredes y tablas de enrutamiento. Dentro de una VPC, se pueden crear subredes en una zona de disponibilidad. Cada subred puede tener una tabla de enrutamiento asociada que define las reglas de direccionamiento para administrar las rutas que toma el tráfico dentro de la subred. Se puede definir una subred que se pueda dirigir a Internet conectando una ruta que vaya a una gateway de Internet o de conversión de las direcciones de red (NAT) asociada a la VPC, o a través de otra VPC.

Cuando se lanza una instancia, una base de datos de RDS u otro servicio dentro de una VPC, este componente tendrá su propio grupo de seguridad por interfaz de red. Este firewall está por fuera de la capa del sistema operativo y se puede utilizar para definir las reglas sobre el tráfico de entrada y salida permitido. También se pueden definir relaciones entre los grupos de seguridad. Por ejemplo, las instancias de un grupo de seguridad del nivel de base de datos solo aceptan el tráfico de las instancias del nivel de aplicación, por referencia a los grupos de seguridad aplicados a las instancias involucradas. A menos que se utilicen protocolos que no sean TCP, no debería ser necesario tener una instancia EC2 a la que se pueda acceder directamente a través de Internet (incluso con puertos restringidos por grupos de seguridad) sin un balanceador de carga o CloudFront. Esto ayuda a evitar accesos no deseados a través de un problema de sistema operativo o aplicación. Una subred también puede tener una ACL de red asociada, que actúe como un firewall sin estado. La ACL de red se debe configurar para reducir el alcance del tráfico permitido entre las capas. Tenga en cuenta que es necesario definir las reglas de entrada y salida.

Mientras que algunos servicios de AWS requieren componentes para acceder a Internet a la hora de hacer llamadas a la API (que es donde se encuentran los puntos de enlace de la API de AWS), otros utilizan puntos de enlace dentro de las VPC. Muchos servicios de AWS, como Amazon S3 y DynamoDB, admiten los puntos de enlace de la VPC, una tecnología que se ha generalizado en AWS PrivateLink. Para los recursos de VPC que necesitan establecer conexiones salientes a Internet, estas se pueden hacer solo de salida (una sola vía) a través de una gateway NAT administrada por AWS, una gateway de Internet solo de salida o proxies web creados y administrados por usted.

Implemente la inspección y la protección: inspeccione y filtre el tráfico en todas las capas. Para los componentes que operan a través de protocolos basados en HTTP, un firewall de aplicación web puede ayudar en materia de protección contra ataques comunes. AWS WAF es un firewall de aplicaciones web que permite monitorear y bloquear solicitudes HTTP(s) que coincidan con sus reglas configurables, las cuales se reenvían a una API de Amazon API Gateway, Amazon CloudFront o un balanceador de carga de aplicaciones. Para comenzar a utilizar AWS WAF, puede utilizar las reglas administradas de AWS en combinación con sus propias reglas, así como las integraciones de socios existentes.

Para administrar las protecciones de AWS Shield Advanced, AWS WAF y los grupos de seguridad de Amazon VPC en AWS Organizations, se puede utilizar AWS Firewall Manager. Le permite configurar y administrar de forma centralizada las reglas del firewall en todas las cuentas y las aplicaciones, lo que facilita ampliar la aplicación de reglas comunes. También le permite responder rápidamente ante ataques, mediante AWS Shield Advanced o soluciones que pueden bloquear de manera automática las solicitudes no deseadas realizadas a sus aplicaciones web.

Automatice la protección de la red: automatice los mecanismos de protección para obtener una red capaz de defenderse a sí misma, basada en la inteligencia sobre amenazas y la detección de anomalías. Por ejemplo, herramientas de detección y prevención de intrusiones que pueden adaptarse a las amenazas actuales y reducir su impacto. Los firewall de aplicaciones web son un ejemplo de cómo se puede automatizar la protección de la red, por ejemplo, mediante la solución AWS WAF Security Automations (https://github.com/awslabs/aws-waf-security-automations) a fin de bloquear automáticamente las solicitudes procedentes de direcciones IP asociadas a agentes de amenaza conocidos.

Recursos

Consulte los siguientes recursos a fin de obtener más información acerca de las prácticas recomendadas de AWS para la protección de las redes.

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

Documentación

- Documentación sobre Amazon VPC
- Introducción a AWS WAF

- Listas de control de acceso de red
- Grupos de seguridad para la VPC
- Reglas de ACL de red recomendadas para la VPC
- AWS Firewall Manager
- AWS PrivateLink
- Puntos de enlace de la VPC
- Amazon Inspector

Práctica

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

Protección de recursos informáticos

Administre las vulnerabilidades: analice y aplique parches con frecuencia para detectar las vulnerabilidades en el código, las dependencias y la infraestructura a fin de facilitar la protección contra nuevas amenazas.

Mediante una canalización de creación e implementación, se pueden automatizar muchas áreas de la administración de vulnerabilidades:

- Utilice herramientas para el análisis de código estático de terceros a fin de identificar problemas de seguridad comunes, como los límites de entrada de funciones no comprobados, así como las vulnerabilidades y las exposiciones comunes (CVE) más recientes. Puede utilizar Amazon CodeGuru para los lenguajes compatibles.
- Utilice herramientas de comprobación de dependencia de terceros a fin de determinar si las bibliotecas vinculadas al código son las últimas versiones, están libres de CVE y tienen condiciones de licencia que cumplen los requisitos de la política de software.
- Mediante Amazon Inspector, se pueden realizar evaluaciones de la configuración de las instancias para detectar vulnerabilidades y exposiciones comunes (CVE) conocidas, compararlas con los puntos de referencia de seguridad y automatizar completamente la notificación sobre defectos. Amazon Inspector se ejecuta en instancias de producción o en una canalización de creación, y notifica a los desarrolladores y los ingenieros cuando hay hallazgos. Se puede obtener acceso a los hallazgos mediante programación y dirigir al equipo a los sistemas de seguimiento de errores y de lista de tareas pendientes. El creador de imágenes EC2 se puede utilizar para mantener las imágenes de servidor (AMI) con implementación automatizada de parches, la aplicación de políticas de seguridad proporcionadas por AWS y otras personalizaciones.

- Cuando utilice contenedores, implemente el escaneo de imágenes ECR en la canalización de creación y regularmente en el repositorio de imágenes para buscar CVE en los contenedores.
- Si bien Amazon Inspector y otras herramientas son eficaces para identificar las configuraciones y cualquier CVE que estén presentes, se requieren otros métodos para probar la carga de trabajo a nivel de aplicación. Fuzzing es un método conocido que sirve para encontrar errores usando la automatización a fin de inyectar datos con formato defectuoso en los campos de entrada y en otras áreas de la aplicación.

Varias de estas funciones se pueden realizar mediante servicios de AWS, productos de AWS Marketplace o herramientas de código abierto.

Reduzca la superficie expuesta a ataques: reduzca la superficie expuesta a ataques mediante el refuerzo de los sistemas operativos, la minimización de los componentes, las bibliotecas y los servicios que se puedan consumir en el exterior y que estén en uso. Para reducir la superficie expuesta a ataques, se necesita un modelo de amenaza que permita la identificación de los puntos de entrada y las amenazas potenciales que podrían surgir. Una práctica común para reducir la superficie expuesta a ataques es empezar por reducir la cantidad de componentes que no se utilizan, ya sean paquetes de sistemas operativos, aplicaciones, etc. (para las cargas de trabajo basadas en EC2) o módulos de software externos en su código (para todas las cargas de trabajo). Existen muchas guías sobre el refuerzo y la configuración de la seguridad para software de servidores y sistemas operativos comunes, por ejemplo, la del Center for Internet Security que puede utilizar como punto de partida y desde ahí iterar.

Permita a las personas realizar acciones a distancia: eliminar la capacidad de acceso interactivo reduce el riesgo de error humano y la posibilidad de configuración o administración manuales. Por ejemplo, utilice un flujo de trabajo de administración de cambios para gestionar las instancias EC2 mediante herramientas, como AWS Systems Manager, en lugar de permitir el acceso directo o a través de un host bastión. AWS Systems Manager puede automatizar distintas tareas de mantenimiento e implementación. Para ello, utiliza características, como flujos de trabajo de automatización, documentos (manuales de identificación de problemas) y el comando de ejecución. Las pilas de AWS CloudFormation crean a partir de las canalizaciones y pueden automatizar la implementación de la infraestructura y las tareas de administración sin utilizar directamente la consola de administración de AWS o las API.

Implemente servicios administrados: implemente servicios que administren los recursos, como Amazon RDS, AWS Lambda y Amazon ECS, a fin de reducir la cantidad de tareas de mantenimiento de la seguridad en el marco del modelo de responsabilidad compartida. Por ejemplo, Amazon RDS lo ayuda a configurar, operar y escalar una base de datos relacional, automatiza las tareas de administración, como el aprovisionamiento de hardware, la configuración de la base de datos, la implementación de parches y la creación de copias de seguridad. Esto se traduce en más tiempo libre para dedicarse a proteger la aplicación de otras formas descritas en el Marco de Buena Arquitectura de AWS. AWS Lambda le permite ejecutar código sin aprovisionar ni administrar servidores, por lo que solo debe centrarse en la

conectividad, la invocación y la seguridad a nivel de código, y no en la infraestructura o el sistema operativo.

Valide la integridad del software: implemente mecanismos (p. ej., la firma de código) para validar que el software, el código y las bibliotecas utilizados en la carga de trabajo provengan de fuentes confiables y no hayan sido manipulados. Por ejemplo, se debe verificar el certificado de firma de código de los binarios y los scripts para confirmar el autor y asegurarse de que no se haya manipulado desde que el autor lo creó. Además, una suma de comprobación del software que se descarga, comparada con la suma de comprobación del proveedor, puede ayudar a garantizar que el software no se haya manipulado.

Automatice la protección informática: automatice los mecanismos informáticos de protección, incluida la administración de vulnerabilidades, la reducción de la superficie expuesta a ataques y la administración de recursos. La automatización permite invertir tiempo en proteger otros aspectos de la carga de trabajo y reduce el riesgo de error humano.

Recursos

Consulte los siguientes recursos a fin de obtener más información sobre las prácticas recomendadas de AWS para la protección de los recursos informáticos.

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

Documentación

- Información general sobre la seguridad de AWS Lambda
- Seguridad en Amazon EC2
- AWS Systems Manager
- Amazon Inspector
- Writing your own AWS Systems Manager documents
- Replacing a Bastion Host with Amazon EC2 Systems Manager

Práctica

- Laboratorio: Automated Deployment of EC2 Web Application

Protección de los datos

Antes de diseñar la arquitectura de cualquier carga de trabajo, se deben establecer prácticas fundamentales que incidan en la seguridad. Por ejemplo, la clasificación de los datos permite categorizarlos en función del nivel de confidencialidad, y el cifrado protege los datos convirtiéndolos en ininteligibles para el acceso no autorizado. Estos métodos son importantes porque respaldan objetivos, como la prevención de la manipulación indebida o la conformidad con las obligaciones normativas.

En AWS, existen varios enfoques diferentes que puede utilizar a la hora de abordar la protección de los datos. En la siguiente sección, se explica cómo utilizar estos enfoques:

- Clasificación de los datos
- Protección de los datos en reposo
- Protección de los datos en tránsito

Clasificación de los datos

La clasificación de datos proporciona una forma de categorizar los datos de la organización en función de la criticidad y la confidencialidad, a fin de determinar los controles de protección y retención adecuados.

Identifique los datos en su carga de trabajo: debe comprender el tipo y la clasificación de los datos que la carga de trabajo procesa, los procesos empresariales asociados, el propietario de los datos, los requisitos legales y de conformidad aplicables, el lugar de almacenamiento y los controles consecuentes que se deben aplicar. Esto puede incluir clasificaciones que indiquen si los datos son de acceso público o exclusivamente de uso interno, como la información de identificación personal (PII) del cliente, así como si los datos son de acceso más restringido, como la propiedad intelectual, la información legalmente privilegiada o marcada como confidencial, entre otras categorías. Mediante la administración cuidadosa de un sistema idóneo de clasificación de datos, junto con los requisitos de nivel de protección de cada carga de trabajo, se pueden trazar los controles y el nivel de acceso o protección adecuado para los datos. Por ejemplo, el contenido público está disponible para que cualquier persona obtenga acceso a él, pero el contenido importante se cifra y se almacena de una manera protegida que exige el acceso autorizado a una clave para descifrar el contenido.

Defina los controles de protección de los datos: mediante el uso de las etiquetas de recursos, cuentas distintas de AWS según la confidencialidad (y potencialmente también en función de la advertencia, el enclave y la comunidad de interés), las políticas de IAM, las políticas de control de servicios (SCP) de las organizaciones, el servicio AWS KMS y AWS CloudHSM, puede definir e implementar las políticas de clasificación y protección de datos con cifrado. Por ejemplo, si tiene un proyecto con buckets de S3 que contienen datos altamente críticos o instancias EC2 que procesan datos confidenciales, estos pueden etiquetarse con “Project=ABC”. Únicamente su equipo inmediato conoce el significado del

código del proyecto. Además, ofrece una forma de usar el control de acceso basado en atributos. Puede definir los niveles de acceso a las claves de cifrado de AWS KMS mediante las políticas y las concesiones de claves para garantizar que solo los servicios adecuados tengan acceso al contenido confidencial a través de un mecanismo seguro. Si toma decisiones de autorización basadas en las etiquetas, debe asegurarse de que los permisos de las etiquetas se definan adecuadamente mediante las políticas de etiquetas de AWS Organizations.

Defina la administración del ciclo de vida de los datos: la estrategia de ciclo de vida que defina debe basarse en el nivel de confidencialidad, así como también en los requisitos legales y de la organización. Se deben tener en cuenta aspectos como el periodo de conservación, los procesos de destrucción, la administración del acceso, la transformación y el intercambio de datos. Se debe encontrar un equilibrio entre la utilidad y el acceso a los datos al momento de elegir una metodología de clasificación de datos. También debe considerar los diferentes niveles de acceso y los matices para implementar un enfoque seguro, pero aun así utilizable para cada nivel. Siempre utilice un enfoque de defensa profundo y reduzca el acceso humano a los datos y a los mecanismos para transformar, eliminar o copiar los datos. Por ejemplo, exija a los usuarios que se autentiquen rigurosamente en una aplicación y otorgue a la aplicación, en lugar de a los usuarios, el permiso de acceso necesario para realizar una "acción a distancia". Además, asegúrese de que los usuarios proceden de una ruta de red de confianza y necesiten obtener acceso a las claves de descifrado. Utilice herramientas como los paneles y los informes automatizados a fin de brindar a los usuarios información sobre los datos en lugar de acceso directo a ellos.

Automatice la identificación y la clasificación de datos: la automatización de la identificación y la clasificación de los datos facilita la implementación de los controles adecuados. En lugar de otorgar acceso directo a una persona, el uso de la automatización para este fin reduce el riesgo de la exposición y de los errores humanos. Debería considerar la utilización de una herramienta como Amazon Macie, que utiliza el aprendizaje automático para localizar, clasificar y proteger de forma automática los datos confidenciales en AWS. Amazon Macie reconoce los datos confidenciales, como la información de identificación personal (PII) o la propiedad intelectual. Además, proporciona paneles y alertas que permiten visualizar cómo se accede a los datos o cómo se trasladan.

Recursos

Para obtener más información acerca de la clasificación de datos, consulte los siguientes recursos.

Documentación

- Documento técnico acerca de la clasificación de datos
- Etiquetado de los recursos de Amazon EC2
- Etiquetado de objetos de Amazon S3

Protección de los datos en reposo

Los datos en reposo son aquellos datos que permanecen en un almacenamiento no volátil a lo largo del tiempo en su carga de trabajo. Esto incluye el almacenamiento por bloques, el almacenamiento de objetos, las bases de datos, los archivos, los dispositivos de IoT y cualquier otro medio de almacenamiento en el que se conserven los datos. La protección de los datos en reposo reduce el riesgo de acceso no autorizado cuando se aplican el cifrado y los controles de acceso adecuados.

El cifrado y la tokenización son dos sistemas de protección de datos fundamentales, pero diferentes.

La *tokenización* es un proceso que permite definir un token para representar información confidencial (por ejemplo, un token para representar el número de la tarjeta de crédito de un cliente). Un token debe carecer de sentido por sí mismo y no debe derivar de los datos que se emplearán para el token; por lo tanto, un valor criptográfico no se puede utilizar como token. Mediante la planificación cuidadosa del enfoque de tokenización, puede proporcionar mayor protección a su contenido y garantizar que se cumplan los requisitos de conformidad. Por ejemplo, si utiliza un token en lugar de un número de tarjeta de crédito, puede reducir el alcance de la conformidad de un sistema de procesamiento de tarjetas de crédito.

El *cifrado* es una forma de transformar el contenido a un modo ilegible sin necesidad de utilizar una clave secreta para descifrar el contenido en un archivo de texto llano. Tanto la tokenización como el cifrado se pueden utilizar para proteger la información según corresponda. Además, el enmascaramiento es una técnica que permite suprimir una parte de los datos hasta el punto en el que los datos restantes no se consideran confidenciales. Por ejemplo, el estándar de seguridad de datos para la industria de tarjetas de pago (PCI-DSS) permite que los últimos cuatro dígitos de un número de tarjeta se mantengan fuera del límite del alcance de conformidad para la indexación.

Implemente una administración de claves segura: defina un enfoque de cifrado que incluya el almacenamiento, la rotación y el control de acceso de las claves para proporcionar la protección necesaria al contenido frente a aquellos usuarios no autorizados y a la exposición innecesaria a usuarios autorizados. AWS KMS le proporciona la ayuda necesaria para administrar las claves de cifrado y se integra con varios servicios de AWS. Este servicio proporciona un almacenamiento duradero, seguro y redundante para las claves maestras. Puede definir los alias de clave, así como las políticas a nivel de clave. Las políticas le ayudan a definir los administradores de clave, así como también los usuarios de dichas claves. Además, AWS CloudHSM es un módulo de seguridad de hardware basado en la nube (HSM) que le permite generar y utilizar fácilmente sus propias claves de cifrado en la nube de AWS. Le ayuda a cumplir con los requisitos de conformidad corporativa, contractual y regulatoria para la seguridad de los datos mediante el uso de los HSM validados por los estándares federales de procesamiento de la información (FIPS) 140-2, nivel 3.

Implemente el cifrado en reposo: debe asegurarse de que la única forma de almacenar datos sea mediante el cifrado. AWS KMS se integra sin problemas con varios de los servicios de AWS para facilitarle el cifrado de los datos en reposo. Por ejemplo, en Amazon S3, puede configurar un cifrado predeterminado en un bucket, de forma que todos los objetos nuevos se cifren automáticamente. Además, Amazon EC2 admite la implementación del cifrado mediante la configuración de una opción de cifrado predeterminado para toda una región.

Aplique el control de acceso: los diferentes controles, como el acceso (de privilegio mínimo), las copias de seguridad (consulte el documento técnico sobre fiabilidad), el aislamiento y el control de versiones, pueden ser de gran ayuda en la protección de sus datos en reposo. El acceso a los datos se debe auditar a través de los mecanismos de detección mencionados anteriormente en este documento técnico, incluido CloudTrail, y los registros de nivel de servicios, como los registros de acceso de S3. Debe realizar un inventario de los datos que son de acceso público y planificar la forma en que puede reducir la cantidad de datos disponibles a lo largo del tiempo. El bloqueo de los almacenes de Amazon S3 Glacier y de los objetos de S3 son capacidades que proporcionan un control de acceso obligatorio. Cuando la política de almacén se bloquea con la opción de conformidad, ni siquiera el usuario raíz puede efectuar cambios en ella, sino hasta que el bloqueo caduque. El mecanismo cumple con los requisitos de administración de libros y registros de SEC, CFTC y FINRA. Para obtener más información al respecto, consulte este documento técnico.

Audite el uso de las claves de cifrado: asegúrese de comprender y auditar el uso de las claves de cifrado para validar que los mecanismos de control de acceso de las claves se implementen de forma adecuada. Por ejemplo, cualquier servicio de AWS que utiliza una clave de AWS KMS registra cada uso en AWS CloudTrail. De esta forma, puede consultar AWS CloudTrail a través de una herramienta como Amazon CloudWatch Insights a fin de asegurarse de que todos los usos de las claves sean válidos.

Utilice mecanismos para mantener a las personas alejadas de los datos: mantenga a todos los usuarios alejados del acceso directo a los datos y los sistemas confidenciales en circunstancias operativas normales. Por ejemplo, utilice un flujo de trabajo de administración de cambios para administrar las instancias EC2 a través de herramientas, en lugar de permitir el acceso directo o un host bastión. Esto se puede lograr con AWS Systems Manager Automation. Este servicio utiliza documentos de automatización que contienen los pasos necesarios para realizar las tareas. Estos documentos se pueden almacenar en el control de origen. Además, se pueden someter a una revisión por pares antes de su ejecución y se pueden probar completamente para minimizar el riesgo en comparación con el acceso shell. Los usuarios empresariales podrían contar con un panel, en lugar de tener acceso directo a un almacén de datos para realizar las consultas. En los casos en que no se utilicen canalizaciones de CI/CD, determine qué controles y procesos se requieren para proporcionar adecuadamente un mecanismo de acceso de emergencia “break-glass” normalmente desactivado.

Automatice la protección de los datos en reposo: utilice herramientas automatizadas para validar e implementar los controles de datos en reposo de forma continua. Por ejemplo,

verifique que solo haya recursos de almacenamiento cifrados. Puede automatizar la validación de que todos los volúmenes de EBS estén cifrados mediante las reglas de AWS Config. AWS Security Hub también puede verificar una serie de controles diferentes a través de las comprobaciones automatizadas de los estándares de seguridad. Además, las reglas de AWS Config pueden corregir automáticamente los recursos que no cumplan con los requisitos.

Recursos

Para obtener más información acerca de las prácticas recomendadas de AWS sobre la protección de los datos en reposo, consulte los siguientes recursos.

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

Documentación

- Protección de datos de Amazon S3 mediante el cifrado
- Cifrado de Amazon EBS
- Cifrado de los recursos de Amazon RDS
- Protección de los datos mediante el cifrado
- Cómo los servicios de AWS utilizan AWS KMS
- Cifrado de Amazon EBS
- AWS Key Management Service
- AWS CloudHSM
- Documento técnico sobre los detalles criptográficos de AWS KMS
- Uso de políticas de clave en AWS KMS
- Uso de políticas de bucket y de usuario
- AWS Crypto Tools

Protección de los datos en tránsito

Los datos en tránsito son todos aquellos datos que se envían de un sistema a otro. Esto incluye la comunicación entre los recursos dentro de la carga de trabajo, así como también la comunicación entre otros servicios y los usuarios finales. Si proporciona el nivel adecuado de protección de los datos en tránsito, protege la confidencialidad y la integridad de los datos de la carga de trabajo.

Implemente una administración segura de claves y certificados: almacene las claves de cifrado y los certificados de forma segura y realice rotaciones de ellos cada cierto tiempo, según corresponda, con un estricto control de acceso. La mejor manera hacerlo es mediante el uso de un servicio administrado, como AWS Certificate Manager (ACM). Este servicio le permite aprovisionar, administrar e implementar fácilmente los certificados de Transport Layer Security (TLS) públicos y privados para su uso con los servicios de AWS y los recursos internos conectados. Los certificados de TLS se utilizan para asegurar las comunicaciones de la red y establecer la identidad de los sitios web en Internet, así como también los recursos de las redes privadas. ACM se integra con los recursos de AWS, como los balanceadores de carga elásticos, las distribuciones de Amazon CloudFront y las API de API Gateway. Además, se encarga de la renovación automática de los certificados. Si utiliza ACM para implementar una autoridad de certificación (CA) de raíz privada, la autoridad de certificación puede proporcionar los certificados y las claves privadas para su uso en las instancias EC2, los contenedores, etc.

Implemente el cifrado en tránsito: implemente los requisitos de cifrado definidos en función de las recomendaciones y los estándares adecuados para que lo ayuden a cumplir los requisitos organizacionales, legales y de conformidad. Los servicios de AWS proporcionan puntos de enlace HTTPS mediante TLS para la comunicación, lo que proporciona un cifrado en tránsito cuando se comunica con las API de AWS. Los protocolos inseguros, como HTTP, se pueden auditar y bloquear en una VPC mediante el uso de grupos de seguridad. Las solicitudes HTTP también se pueden redirigir automáticamente a HTTPS en Amazon CloudFront o en un balanceador de carga de aplicaciones. Tiene control total sobre los recursos informáticos para implementar el cifrado en tránsito en los servicios. Además, puede utilizar la conectividad de VPN en la VPC desde una red externa para facilitar el cifrado del tráfico. En caso de tener requerimientos especiales, las soluciones de terceros están disponibles en AWS Marketplace.

Autentique las comunicaciones de red: el uso de protocolos de red que admiten la autenticación permite establecer la confianza entre las partes. Esto se suma al cifrado utilizado en el protocolo para reducir el riesgo de que las comunicaciones se alteren o intercepten. Entre los protocolos comunes que implementan la autenticación, se incluye el protocolo de Transport Layer Security (TLS), que se utiliza en varios servicios de AWS, y el protocolo IPsec, que se utiliza en AWS Virtual Private Network (AWS VPN).

Automatice la detección del acceso no intencionado a los datos: utilice herramientas como Amazon GuardDuty para detectar automáticamente los intentos de trasladar datos fuera de los límites definidos en función del nivel de clasificación de los datos. Por ejemplo, detectar un troyano que copia datos a una red desconocida o no confiable mediante el protocolo DNS. Además de Amazon GuardDuty, se pueden utilizar los registros de flujo de Amazon VPC, que registran la información del tráfico de la red, junto con Amazon EventBridge para activar la detección de conexiones anormales, tanto las conexiones exitosas como las denegadas. El analizador de acceso para S3 puede ayudarlo a evaluar quiénes pueden acceder a qué datos en sus buckets de S3.

Recursos

Para obtener más información acerca de las prácticas recomendadas de AWS sobre la protección de los datos en tránsito, consulte los siguientes recursos.

Video

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

Documentación

- AWS Certificate Manager
- Agentes de escucha de HTTPS para el balanceador de carga de aplicaciones
- AWS VPN
- API Gateway optimizada para bordes

Respuesta ante incidentes

Incluso si cuenta con controles preventivos y de detección extremadamente maduros, su organización debe implementar mecanismos para responder al posible impacto de los incidentes de seguridad y mitigarlos. Su nivel de preparación incide de forma significativa en la capacidad de los equipos para operar efectivamente durante un incidente, aislar y contener los problemas, así como también para restablecer las operaciones a un buen estado conocido. Establecer las herramientas y el acceso antes de un incidente de seguridad y, luego, practicar a modo de rutina la respuesta ante incidentes durante los días de prueba resulta sumamente útil para garantizar su recuperación, mientras minimiza las interrupciones que se produjeron en su empresa.

Objetivos de diseño de la respuesta de la nube

Aunque los procesos y los mecanismos generales de respuesta ante incidentes, como aquellos que se definen en NIST 800-61 de la Guía para la gestión de incidentes de seguridad informática, permanecen vigentes, recomendamos evaluar estas metas de diseño específicas que son relevantes para responder a los incidentes de seguridad en un entorno en la nube:

- **Establezca objetivos de respuesta:** trabaje de forma conjunta con las partes interesadas, los asesores jurídicos y los líderes de la organización para determinar el objetivo de la respuesta ante un incidente. Algunos objetivos comunes son la contención y la mitigación del problema, la recuperación de los recursos afectados, la preservación de los datos para llevar a cabo los análisis forenses correspondientes y la atribución.
- **Documente los planes:** cree planes que lo ayuden con la respuesta ante un incidente, con la comunicación y su posterior recuperación.
- **Responda a través de la nube:** implemente sus patrones de respuesta en donde se presente la situación.
- **Conozca lo que tiene y lo que necesita:** conserve los registros, las instantáneas y otras pruebas. Para ello, cópielos en una cuenta de seguridad centralizada en la nube. Utilice las etiquetas, los metadatos y los mecanismos que implementan las políticas de retención. Por ejemplo, puede elegir el comando dd de Linux o un comando equivalente de Windows a fin de realizar una copia completa de los datos para investigar.
- **Utilice mecanismos para repetir la implementación:** si considera que una cierta anomalía de seguridad se puede atribuir a una configuración errónea, es posible que la corrección sea tan simple como eliminar la variación y volver a implementar los recursos con la configuración adecuada. Cuando sea posible, haga que los mecanismos de respuesta sean lo suficientemente seguros como para que se ejecuten en más de una ocasión y en entornos que se encuentren en un estado desconocido.

- **Automatice cuando sea posible:** cuando note que los problemas o los incidentes se repiten, desarrolle mecanismos que analicen y respondan mediante programación a situaciones comunes. Utilice las respuestas humanas ante incidentes únicos, nuevos y delicados.
- **Elija soluciones escalables:** esfuércese por igualar la escalabilidad del enfoque de la organización a la informática en la nube y reduzca el tiempo entre la detección y la respuesta.
- **Aprenda y mejore el proceso:** cuando identifique desfases en el proceso, las herramientas o las personas, elabore planes para solucionarlos. Las simulaciones son métodos seguros para detectar dichos desfases y mejorar los procesos.

En AWS, existe una serie de enfoques diferentes que se pueden utilizar para abordar la respuesta ante incidentes. En la siguiente sección, se explica cómo utilizar estos enfoques:

- **Capacite** a su personal de operaciones de seguridad y de respuesta ante incidentes sobre las tecnologías de la nube y cómo la organización pretende utilizarlas.
- **Prepare** a su equipo de respuesta ante incidentes para detectar y responder ante incidentes en la nube, active las capacidades de detección y garantice el acceso adecuado a las herramientas y los servicios de la nube necesarios. Además, prepare los manuales de procedimientos necesarios, tanto manuales como automatizados, a fin de garantizar respuestas coherentes y de confianza. Trabaje junto con otros equipos para establecer las operaciones de referencia esperadas y utilice esos conocimientos a fin de identificar las desviaciones de esas operaciones normales.
- **Simule** eventos de seguridad esperados e inesperados dentro de su entorno de la nube para comprender la efectividad de su preparación.
- **Itere** el resultado de su simulación para mejorar la escala de la posición de su respuesta, reducir el tiempo de creación de valor y disminuir aún más el riesgo.

Eduque

Los procesos automatizados permiten a las organizaciones dedicar más tiempo a las medidas para aumentar la seguridad de sus cargas de trabajo. La respuesta automatizada ante incidentes también permite que las personas estén disponibles para identificar aquellos eventos relacionados, practicar simulaciones, idear nuevos procedimientos de respuesta, realizar investigaciones, desarrollar nuevas habilidades y probar o crear nuevas herramientas. A pesar del aumento en materia de automatización, el equipo, los especialistas y quienes responden dentro de una organización de seguridad deben recibir educación constantemente.

Más allá de la experiencia general en la nube, debe invertir considerablemente en el personal para tener éxito. Su organización se puede beneficiar a través de la capacitación adicional que

brinde al personal sobre las habilidades de programación, los procesos de desarrollo (incluidos los sistemas de control de versiones y las prácticas de implementación) y la automatización de la infraestructura. La mejor manera de aprender es a través de la práctica, es decir, a través de los días de prueba de respuesta ante incidentes. Esto permite a los expertos del equipo perfeccionar las herramientas y las técnicas, a la vez que enseñan a los demás.

Prepare

Durante un incidente, sus equipos de respuesta ante incidentes deben tener acceso a las diferentes herramientas y los recursos de la carga de trabajo implicados. Asegúrese de que los equipos cuenten con un acceso aprovisionado previamente para que puedan realizar sus tareas antes de que ocurra el evento. Todas las herramientas, el acceso y los planes se deben documentar y probar antes de que ocurra un evento a fin de garantizar que pueden brindar una respuesta oportuna.

Identifique al personal clave y a los recursos externos: cuando define el enfoque que seguirá con respecto a la respuesta ante incidentes en la nube junto con otros equipos (como su asesor jurídico, liderazgo, las partes interesadas de la empresa, los servicios de AWS Support, entre otros), debe identificar al personal clave, a las partes interesadas y a los contactos pertinentes. Para reducir la dependencia y disminuir el tiempo de respuesta, asegúrese de que su equipo, los equipos de seguridad especializados y quienes responden reciban la educación necesaria sobre los servicios que se utilizan y tengan oportunidades suficientes para practicar lo que hayan aprendido.

Recomendamos que identifique a los socios de seguridad externos de AWS que puedan compartir su experiencia en el ámbito y puedan también aportar una perspectiva diferente a fin de aumentar la capacidad de respuesta. Los socios de confianza en materia de seguridad pueden ser de gran ayuda en la identificación de los posibles riesgos o las amenazas que desconozca.

Desarrolle planes de administración de incidentes: elabore planes que le ayuden a responder ante incidentes, a comunicarse durante ellos y a recuperarse luego. Por ejemplo, puede comenzar con la planificación de las respuestas ante incidentes a través de las situaciones más probables que podrían afrontar su carga de trabajo y su organización. Incluya la forma en que se comunicaría durante el incidente y cómo escalaría tanto interna como externamente. Cree planes de respuesta ante incidentes en forma de manuales de estrategias. Comience con las situaciones más probables que podrían afrontar su carga de trabajo y su organización. Pueden ser eventos que se generen en la actualidad. Si necesita un punto de partida, considere los hallazgos de AWS Trusted Advisor y Amazon GuardDuty. Utilice un formato sencillo, como un markdown, para que sea fácil de mantener, pero asegúrese de que se incluyan los comandos o los fragmentos de código importantes, de forma que se puedan ejecutar sin tener que consultar otra documentación.

Comience de forma simple e itere. Trabaje en estrecha colaboración con los socios y los expertos en seguridad para identificar las tareas necesarias a fin de garantizar que los procesos

sean posibles. Defina las descripciones manuales de los procesos que realiza. A continuación, pruebe los procesos e itere el patrón del manual de procedimientos para mejorar la lógica central de la respuesta. Determine cuáles son las excepciones y cuáles son las resoluciones alternativas en esos casos. Por ejemplo, en un entorno de desarrollo, es posible que desee terminar una instancia mal configurada de Amazon EC2. Sin embargo, si el mismo evento se presenta en un entorno de producción, en lugar de terminar la instancia, podría detener la instancia y verificar junto con las partes interesadas que no se perderán los datos críticos y que la terminación es aceptable. Incluya la forma en que se comunicaría durante el incidente y cómo escalaría tanto interna como externamente. Cuando se sienta cómodo con la respuesta manual del proceso, automatice la respuesta para reducir el tiempo de resolución.

Aprovisione el acceso previamente: asegúrese de que quienes responden ante los incidentes cuenten con el acceso correcto a los sistemas de AWS y otros sistemas relevantes. Este acceso se debe aprovisionar previamente a fin de reducir el tiempo que transcurre desde la investigación hasta la recuperación. Determinar cómo facilitar el acceso a las personas adecuadas durante un incidente retrasa el tiempo necesario para responder y puede causar otras deficiencias en materia de seguridad si el acceso se comparte o no se suministra adecuadamente mientras se está bajo presión. Debe saber qué nivel de acceso requieren los miembros de su equipo (por ejemplo, qué tipo de acciones es probable que realicen) y debe aprovisionar el acceso con antelación. El acceso en forma de roles o usuarios creados específicamente para responder ante un incidente de seguridad se suele privilegiar a fin de proporcionar un acceso suficiente. Por lo tanto, se debe restringir el uso de esas cuentas de usuario. Además, no se deben utilizar para actividades diarias y se debe alertar sobre su uso.

Implemente las herramientas previamente: asegúrese de que el personal de seguridad tenga las herramientas adecuadas previamente implementadas en AWS para reducir el tiempo que transcurre desde la investigación hasta la recuperación.

Para automatizar la ingeniería de seguridad y las funciones de las operaciones, puede utilizar un conjunto completo de API y herramientas de AWS. Puede automatizar completamente la administración de identidades, la seguridad de la red, la protección de los datos y las capacidades de monitoreo, y entregarlas mediante los métodos de desarrollo de software conocidos que ya tiene implementados. Cuando desarrolla la automatización de la seguridad, el sistema puede monitorear, revisar e iniciar una respuesta, en lugar de que las personas monitoreen su posición con respecto a la seguridad y reaccionen manualmente a los eventos.

Si los equipos de respuesta ante incidentes mantienen la misma forma de respuesta ante las alertas, se arriesgan a que se produzca una fatiga de alerta. Con el tiempo, el equipo puede perder la sensibilidad ante las alertas y puede cometer errores en el manejo de situaciones ordinarias o pasar por alto alertas inusuales. La automatización ayuda a evitar la fatiga de alertas mediante el uso de funciones que procesan las alertas repetitivas y ordinarias. Esto permite que las personas se ocupen de los incidentes sensibles y únicos.

Puede mejorar los procesos manuales a través de la automatización mediante programación de los pasos del proceso. Después de definir el patrón de correcciones de un evento, puede descomponer ese patrón en una lógica factible y escribir el código para ejecutar esa lógica. Quienes responden pueden entonces ejecutar ese código para corregir el problema. Con el tiempo, puede automatizar cada vez más pasos y, en última instancia, puede gestionar automáticamente clases enteras de incidentes comunes.

En el caso de las herramientas que se ejecutan dentro del sistema operativo de la instancia EC2, debe considerar la opción de utilizar el comando de ejecución de AWS Systems Manager, que le permite administrar de forma remota y segura las instancias a través de un agente que se instala en el sistema operativo de la instancia de Amazon EC2. Se requiere el agente de AWS Systems Manager (agente de SSM), que se encuentra instalado de forma predeterminada en varias imágenes de Amazon Machine (AMI). Sin embargo, tenga en cuenta que una vez que una instancia fue atacada, ninguna respuesta de las herramientas o los agentes que se ejecutan en ella debe considerarse de confianza.

Prepare las capacidades forenses: identifique y prepare las capacidades de investigación forense que sean adecuadas, incluidos los especialistas externos, las herramientas y la automatización. Algunas de las actividades de respuesta ante incidentes pueden incluir el análisis de imágenes de disco, los sistemas de archivos, los volcados de memoria RAM u otros artefactos que estén implicados en un incidente. Cree una estación de trabajo forense personalizada que se pueda utilizar para montar copias de cualquier volumen de datos afectado. Dado que las técnicas de investigación forense requieren una capacitación técnica, puede que sea necesario contratar a especialistas externos.

Simule

Organice días de prueba: los días de prueba, también conocidos como simulaciones o ejercicios, son eventos internos que ofrecen una oportunidad estructurada para poner en práctica los planes y los procedimientos de administración de incidentes en el contexto de una situación realista. Los días de prueba consisten fundamentalmente en estar preparado y mejorar iterativamente la capacidad de respuesta. Algunas de las razones por las que puede encontrar valor en las actividades que se llevan a cabo en el día de prueba son las siguientes:

- Validar la preparación
- Desarrollar la confianza: aprender a partir de las simulaciones y capacitar al personal
- Cumplir las obligaciones contractuales o de conformidad
- Generar artefactos para la acreditación
- Adquirir agilidad: mejoras graduales
- Adquirir velocidad y mejorar las herramientas

- Perfeccionar la comunicación y el escalado
- Desarrollar confianza ante situaciones extrañas e inesperadas

En consecuencia, el valor que deriva de la participación en una actividad de SIRS aumenta la efectividad de una organización a la hora de afrontar eventos estresantes. El desarrollo de una actividad de SIRS que sea a la vez realista y beneficiosa puede ser un ejercicio difícil. Si bien probar los procedimientos o la automatización que gestiona los eventos sobre los que tenemos una gran comprensión tiene ciertas ventajas, es igual de valioso participar en actividades creativas de SIRS para probarse uno mismo ante situaciones inesperadas y mejorar continuamente.

Itere

Automatice la capacidad de contención y recuperación: automatice la contención y la recuperación de un incidente a fin de reducir los tiempos de respuesta y el impacto que puede causar en la organización.

Una vez que cree y practique los procesos y las herramientas del manual de estrategias, puede descomponer la lógica en una solución basada en código, que aquellos que se encargan de responder ante incidentes pueden utilizar para automatizar la respuesta y eliminar la variación o las suposiciones que les surjan. Esto puede acelerar el ciclo de vida de una respuesta. El siguiente objetivo es permitir que este código se automatice completamente y que las alertas o los eventos mismos lo invoquen, en lugar de la persona que responde, a fin de crear una respuesta basada en eventos.

Con un sistema de respuesta basado en eventos, un mecanismo de detección activa un mecanismo de respuesta para remediar automáticamente el evento. Puede utilizar las capacidades de respuesta basada en eventos para reducir el tiempo de creación de valor entre los mecanismos de detección y los mecanismos de respuesta. Para crear esta arquitectura basada en eventos, puede utilizar AWS Lambda, el cual es un servicio de informática sin servidor que ejecuta su código en respuesta a eventos y administra automáticamente por usted los recursos de informática subyacentes. Por ejemplo, supongamos que tiene una cuenta de AWS con el servicio AWS CloudTrail habilitado. Si alguna vez desactiva AWS CloudTrail (a través de la llamada a la API cloudtrail:StopLogging), puede utilizar Amazon EventBridge para monitorear el evento específico de cloudtrail:StopLogging e invocar una función de AWS Lambda para llamar a cloudtrail:StartLogging a fin de reiniciar el registro.

Recursos

Para obtener más información acerca de las prácticas recomendadas actuales de AWS sobre la respuesta ante incidentes, consulte los siguientes recursos.

Videos

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

Documentación

- Guía de respuesta ante incidentes de AWS
- AWS Step Functions
- Amazon EventBridge
- CloudEndure Disaster Recovery

Práctica

- 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

Conclusión

La seguridad es un esfuerzo constante. Cuando se producen incidentes, deberían considerarse oportunidades para mejorar la seguridad de la arquitectura. Disponer de controles de identidad sólidos, automatizar las respuestas ante eventos de seguridad, proteger la infraestructura en varios niveles y administrar los datos bien clasificados mediante el cifrado proporciona una defensa profunda que toda organización debería implementar. Este esfuerzo es mucho más fácil gracias a las funciones programáticas y a las características y los servicios de AWS que se analizan en este documento.

AWS se esfuerza por ayudarlo a crear y operar arquitecturas que protejan la información, los sistemas y los activos, al tiempo que aportan valor de negocio.

Colaboradores

En este documento, contribuyeron las siguientes personas y organizaciones:

- Ben Potter, líder de seguridad, Well-Architected, Amazon Web Services
- Bill Shinn, director sénior, Oficina de CISO, Amazon Web Services

- Brigid Johnson, directora de desarrollo de software sénior, AWS Identity, Amazon Web Services
- Byron Pogson, arquitecto de soluciones sénior, Amazon Web Services
- Darran Boyd, arquitecto de soluciones de seguridad principal, Servicios financieros, Amazon Web Services
- Dave Walker, arquitecto principal especialista en soluciones, Seguridad y conformidad, Amazon Web Services
- Paul Hawkins, estratega de seguridad sénior, Amazon Web Services
- Sam Elmalak, líder de tecnología sénior, Amazon Web Services

Documentación adicional

Para obtener más información, consulte las siguientes fuentes:

- Documento técnico sobre el Marco de buena arquitectura de AWS

Revisiones del documento

Fecha	Descripción
Julio de 2020	Actualización de la guía en materia de cuentas, identidad y administración de permisos.
Abril de 2020	Actualización para ampliar el asesoramiento en todas las áreas e incluir nuevas prácticas recomendadas, servicios y características.
Julio de 2018	Actualizaciones para reflejar las características y los servicios nuevos de AWS, así como también las referencias actualizadas de
Mayo de 2017	Actualización de la sección de configuración y mantenimiento de la seguridad del sistema para reflejar las características y los
Noviembre de 2016	Primera publicación