COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 2
Principios de diseño para la seguridad

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

TIC

Presiona cada botón para ecceder a más contenido aquí y en el resto de páginas.

7 Principios

de diseño para la seguridad

Marco

Aplicar el principio del mínimo privilegio

Habilitar la trazabilidad

Proteger todas las capas

Automatizar la seguridad

Proteger los datos en tránsito y los datos en reposo

Prepararse para los eventos de seguridad

Minimizar la superficie de ataque

Puntos clave

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Se describen los siete principios de diseño del pilar de seguridad del Marco de AWS Well-Architected. Seguir estos principios puede ayudar a fortalecer la seguridad de su carga de trabajo y puede ayudar a guiar sus conversaciones sobre seguridad y cumplimiento.

COLOMBIA POTENCIA DE LA VIDA

TIC

Aplicar el principio del mínimo privilegio

- Conceder acceso según sea necesario
- Hacer cumplir la división de controles
- Evitar las credenciales a largo plazo

Seguridad | Partes clave | 7 privilegios

Una cultura de seguridad organizacional debe construirse sobre el principio del mínimo privilegio. Solo conceda acceso a los datos y otros recursos a las personas que realmente lo necesitan. Puede comenzar por denegar el acceso a todo y otorgar acceso según sea necesario en función de los roles de trabajo.

Una práctica recomendada de seguridad es hacer cumplir la separación de funciones con la autorización adecuada para cada interacción con sus recursos de AWS. Establezca expectativas sobre cómo se delegará la autoridad a través de los ingenieros de software, el personal de operaciones y otras funciones laborales que están involucradas en la adopción de la nube.

Al reducir o incluso eliminar la dependencia de las credenciales a largo plazo, puede disminuir su área de superficie de ataque. Puede usar credenciales temporales y requerir identidades para adquirirlas dinámicamente. Para las identidades de la fuerza laboral, use AWS Single Sign-On o la federación con IAM para acceder a las cuentas de AWS. Para las identidades de máquinas, como las instancias de EC2

o las funciones de AWS Lambda, se requiere el uso de roles de IAM, en lugar de usuarios de IAM con claves de acceso a largo plazo.

Identity and Access Management son partes clave de un programa de seguridad de la información para garantizar que solo los usuarios y componentes autorizados y autenticados puedan acceder a sus recursos, y solo de la manera que usted desea. En AWS, IAM es el servicio principal para la administración de permisos. El servicio proporciona la capacidad de controlar el acceso programático y de usuarios a los servicios y recursos de AWS.

Con IAM, puede definir entidades principales (es decir, cuentas, usuarios, funciones y servicios que pueden realizar acciones en su cuenta) y desarrollar políticas granulares alineadas con estas entidades. También tiene la capacidad de exigir prácticas sólidas de contraseña, como establecer un nivel de complejidad, evitar la reutilización y hacer cumplir la autenticación multifactor (MFA). Puede usar la federación con su servicio de Directory Service Para las cargas de trabajo que requieren que los sistemas tengan acceso a AWS, IAM puede proporcionar acceso seguro a través de funciones, perfiles de instancia, identidad federada y credenciales temporales.

COLOMBIA POTENCIA DE LA VIDA

TIC

Habilitar la trazabilidad

- Supervisar las acciones y los cambios
- Usar registro y métricas
- Auditar los recursos de la nube

Tiempo real

Detección

7 privilegios

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Con AWS, puede supervisar y auditar las acciones y los cambios en su entorno en tiempo real, y alertar sobre ellos. AWS proporciona registro nativo, así como servicios que puede utilizar para proporcionar una mayor visibilidad casi en tiempo real de las ocurrencias en su entorno. Integre estas herramientas con sus soluciones existentes de registro y supervisión. Conozca qué cargas de trabajo están implementadas y operativas, de modo que pueda auditar y asegurarse de que el entorno esté funcionando en los niveles de gobierno de seguridad esperados y cumpla con los estándares de seguridad requeridos.

En AWS, puede implementar controles de detección procesando registros y eventos, y supervisando, lo que permite la auditoría, el análisis automatizado y las alarmas. Los registros de CloudTrail, las llamadas API de AWS y Amazon CloudWatch brinda supervisión de métricas con alarmas, y AWS Config brinda el historial de configuración. Amazon GuardDuty es un servicio administrado de detección de amenazas que supervisa continuamente comportamientos malintencionados o no autorizados para ayudar a proteger sus cuentas y cargas de trabajo de AWS. Los registros de nivel de servicio también están disponibles; por ejemplo, puede usar Amazon S3 para registrar solicitudes de acceso.

Proteger todas las capas

- Utilizar un enfoque de defensa en profundidad
- Utilizar diferentes servicios de AWS

Controles | Configuración | 7 privilegios

En lugar de centrarse únicamente en la protección de una sola capa exterior, aplique un enfoque de defensa en profundidad con otros controles de seguridad. Esto significa aplicar seguridad a todas las capas, como su red, aplicación y almacén de datos. Por ejemplo, puede solicitar a los usuarios que se autentiquen fuertemente en una aplicación. Además, asegúrese de que los usuarios provengan de una ruta de red confiable y requieran acceso a las claves de descifrado para procesar los datos cifrados. Uno de los beneficios de utilizar AWS es que nuestros servicios también están diseñados para la integración. Puede utilizar varios servicios de AWS juntos a fin de proporcionar el entorno más seguro para sus datos y recursos.

Los clientes de AWS pueden adaptar o reforzar la configuración de una instancia de EC2, un contenedor de Amazon Elastic Container Service (Amazon ECS) o una instancia de AWS Elastic Beanstalk y conservar esta configuración en una imagen de máquina de Amazon (AMI) inmutable. Luego, todos los nuevos servidores virtuales (instancias) lanzados con esta AMI reciben la configuración reforzada, ya sea que se lancen manualmente o mediante escalado automático.

COLOMBIA POTENCIA DE LA VIDA

TIC

Automatizar la seguridad

- Automatizar las tareas de seguridad de rutina con las API
- Implementar infraestructura como código

Software

Entornos

7 privilegios

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

En la nube de AWS, puede convertir su infraestructura en código. Con esta capacidad, puede automatizar la creación de entornos confiables para realizar investigaciones y análisis forenses más profundos. Puede ejecutar simulaciones de respuesta a incidentes y utilizar herramientas con automatización para aumentar la velocidad de la detección, la investigación y la recuperación. Al automatizar las implementaciones y el mantenimiento, puede eliminar el acceso del operador para reducir la superficie de ataque.

AWS desarrolla herramientas de seguridad especialmente diseñadas que pueden ayudarle a automatizar muchas de las tareas rutinarias a las que los expertos en seguridad normalmente dedican tiempo. Esto significa que los expertos en seguridad pueden dedicar más tiempo a centrarse en las medidas para aumentar la seguridad de su entorno en la nube de AWS.

Puede automatizar las funciones de ingeniería y operaciones de seguridad mediante el uso de un conjunto integral de API y herramientas. Puede automatizar por completo la administración de identidades, la seguridad de la red y la protección de datos, y las capacidades de supervisión, y entregarlas mediante el uso de métodos de desarrollo de software populares que ya tiene implementados. En lugar de tener personas que supervisen su posición de seguridad y reaccionen ante un evento, con la automatización, su sistema puede supervisar, revisar e iniciar una respuesta.

COLOMBIA POTENCIA DE LA VIDA

TIC

Proteger los datos en tránsito y los datos en reposo

- Utilizar los controles de acceso y cifrado
- Clasificar los datos con etiquetas
- Aprovechar las conexiones de VPN y TLS

Protección | Funciones | 7 privilegios

AWS proporciona varios medios para cifrar datos en reposo y datos en tránsito. Creamos funciones en nuestros servicios que facilitan el cifrado de sus datos. Por ejemplo, hemos implementado el cifrado del lado del servidor (SSE) para Amazon

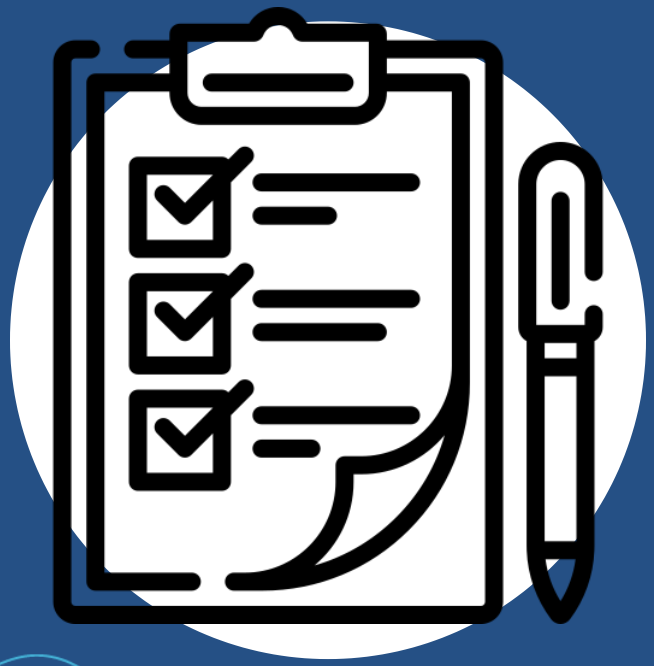
S3 para que le resulte más fácil almacenar sus datos de forma cifrada. También puede hacer arreglos para que **Elastic Load Balancing (ELB)** maneje todo el proceso de cifrado y descifrado de HTTPS (generalmente conocido como terminación SSL).

La protección de los datos es una parte fundamental de la creación y la operación de los sistemas de información. AWS proporciona servicios y características que ayudan a proteger sus datos en reposo y en tránsito. Las medidas de seguridad incluyen controles de acceso detallados a los objetos, la creación y el control de las claves de cifrado que se utilizan para cifrar sus datos, la selección de métodos de cifrado apropiados, la validación de la integridad y la retención de datos adecuada. Para ayudarlo a administrar la protección, implemente un esquema de etiquetado para clasificar sus datos en niveles de confidencialidad. Otra práctica recomendada de seguridad es construir mecanismos para proteger los datos en tránsito, como el uso de conexiones de **red privada virtual (VPN)** y Transport Layer Security (TLS).

COLOMBIA POTENCIA DE LA VIDA

TIC

Prepararse para los eventos de seguridad



- Mitigar el impacto de los incidentes de seguridad
- Crear procesos para aislar los incidentes y restaurar las operaciones

Impacto

Prácticas

7 privilegios

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Incluso con controles preventivos y de detección maduros, debe implementar procesos para responder y mitigar el impacto potencial de los incidentes de seguridad. La arquitectura de la carga de trabajo afecta fuertemente su capacidad de operar de modo eficaz durante un incidente, aislar o contener los sistemas y restaurar las operaciones a un estado correcto conocido. Instale las herramientas y el acceso antes de un incidente de seguridad. Luego, practique rutinariamente la respuesta a incidentes durante los días de juego. Esto lo ayudará a garantizar que su arquitectura pueda adaptarse a una investigación y recuperación oportunas. En otro módulo de este curso, se describe una variedad de enfoques para la respuesta ante incidentes.

En AWS, las siguientes prácticas facilitan una respuesta eficaz ante incidentes:

- El registro detallado está disponible. Los registros contienen contenido importante, como acceso a archivos y cambios.
- Los eventos se pueden procesar automáticamente y pueden invocar herramientas que automaticen las respuestas mediante el uso de las API de AWS.
- Puede preaprovisionar herramientas y una "sala limpia" mediante AWS **CloudFormation**. Esto proporciona la capacidad de llevar a cabo análisis forenses en un entorno seguro y aislado.

Minimizar la superficie de ataque

- Prepararse para escalar y absorber el ataque
- Defender los recursos expuestos

Ciberataque | Infraestructura | 7 privilegios

Ciertos servicios de AWS, como AWS Auto Scaling y Amazon CloudFront, brindan a las aplicaciones la capacidad de escalar para absorber ataques comunes a la capa de infraestructura. Un ataque de reflexión UDP tiene lugar cuando el atacante solicita información al equipo objetivo utilizando una dirección de origen falsificada. Una inundación SYN es un tipo de ataque por denegación de servicio distribuido (DDoS) que tiene como objetivo hacer que un servidor no esté disponible para el tráfico legítimo al consumir todos los recursos disponibles del servidor. Mediante el uso de técnicas como el escalado automático, puede absorber mayores volúmenes de ataques a la capa de aplicación.

Generalmente, un ciberataque se cierra debido a dos razones: o los atacantes se agotan y se dan por vencidos o los atacantes logran su objetivo. Reduzca su exposición al acceso no deseado fortaleciendo los sistemas operativos y minimizando los componentes, las bibliotecas y los servicios consumibles externos en uso. Comience por reducir los componentes no utilizados, como los paquetes y las aplicaciones del sistema operativo. Configure grupos de seguridad y listas de control de acceso a la red (ACL) en Amazon Virtual Private Cloud (Amazon VPC) para ayudar a reducir la superficie de ataque de sus aplicaciones.

Puntos clave

Los puntos clave de esta lección de la unidad son los principios de diseño para la seguridad en la nube:

- Aplicar el principio de mínimo privilegio
- Proteger los datos en tránsito y los datos en reposo
- Habilitar la trazabilidad
- Prepararse para los eventos de seguridad
- Proteger todas las capas
- Minimizar la superficie de ataque
- Automatizar la seguridad

7 privilegios