CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS

DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

UNIVERSIDAD DE GUADALAJARA

Red Universitaria e Institución Benemérita de Jalisco

Seguridad

Sección D04

Profesor: Vazquez Curiel Armida Griselda

04 - 05 - 2024

Autor: Juan Antonio Perez Juarez

Actividad 3.1 Seguridad en Centro de procesamiento de datos

Seguridad en Centro de procesamiento de datos de Amazon Web Services

Introducción

Los Centros de Datos de Amazon Web Services (AWS) son componentes críticos de la infraestructura global de la nube de AWS, que alberga una amplia gama de servicios en la nube utilizados por millones de clientes en todo el mundo. Este manual establece los estándares de seguridad y las mejores prácticas para garantizar la protección de la infraestructura, los datos y la continuidad del servicio en los Centros de Datos de AWS.

Objetivos

• Proteger la integridad, confidencialidad y disponibilidad de la infraestructura y los datos de AWS.

• Cumplir con los estándares de seguridad y privacidad aplicables, incluidos los requisitos de certificación y cumplimiento.

• Mitigar los riesgos de amenazas físicas y cibernéticas que puedan afectar los Centros de Datos de AWS.

• Mantener la confianza de los clientes y las partes interesadas en la seguridad de la infraestructura de AWS.

• AWS sigue un enfoque de "seguridad por diseño" en el desarrollo y mantenimiento de sus centros de datos.

• Se implementan controles de seguridad basados en estándares reconocidos de la industria, como ISO 27001, SOC 2 y PCI DSS.

• Se mantienen políticas y procedimientos de seguridad actualizados y se comunican de manera efectiva a todo el personal relevante.

Acceso Físico

• El acceso físico a los centros de datos de AWS está estrictamente controlado y restringido al personal autorizado.

• Se utilizan medidas de seguridad física, como controles biométricos, cámaras de vigilancia y sistemas de alarma, para proteger las instalaciones.

• Las visitas al centro de datos son supervisadas y se requieren identificaciones válidas para acceder a las áreas restringidas.

Acceso Lógico

• Se implementa un sistema de gestión de identidades y accesos (IAM) para controlar y auditar el acceso lógico a los sistemas y datos de AWS.

• Se aplican políticas de seguridad de contraseñas y autenticación de

múltiples factores para fortalecer la seguridad de las cuentas de usuario.

• Se siguen los principios de "menor privilegio" y "necesidad de saber" para limitar el acceso a la información solo a aquellos que lo necesitan para realizar sus funciones.

Monitoreo y Detección de Intrusiones

• Se emplean herramientas avanzadas de monitoreo y análisis de seguridad para detectar y responder a actividades sospechosas en tiempo real.

• Se establecen alertas automáticas para notificar al personal de seguridad sobre posibles incidentes de seguridad.

• Se realizan análisis de registros y auditorías de seguridad de forma regular para identificar y mitigar posibles vulnerabilidades.

Respuesta a Incidentes

• Se mantiene un plan de respuesta a incidentes detallado y se realizan ejercicios periódicos de simulación para preparar al personal.

• Todos los incidentes de seguridad se reportan de inmediato al equipo de respuesta a incidentes de AWS para su investigación y resolución.

• Se realizan análisis posteriores a los incidentes para identificar lecciones aprendidas y mejorar los controles de seguridad.

Auditorías y Revisiones

• Se someten los centros de datos de AWS a auditorías externas e internas periódicas para evaluar el cumplimiento de los estándares de seguridad.

• Se lleva a cabo una revisión regular de los controles de seguridad y se realizan mejoras según sea necesario para abordar los hallazgos de las auditorías.

• Se proporciona a los clientes la capacidad de realizar auditorías y evaluaciones de seguridad independientes bajo ciertas condiciones.

Resiliencia y Continuidad del Negocio

• Se implementan medidas de resiliencia, como redundancia de sistemas, para garantizar la disponibilidad continua de los servicios de AWS en caso de fallas o desastres.

• Se realizan pruebas periódicas de recuperación ante desastres (DR) para validar la eficacia de los planes y procedimientos de recuperación.

• Se ofrece a los clientes opciones para respaldar y recuperar sus datos de forma segura y eficiente.

Gestión de Cambios

• Se sigue un proceso de gestión de cambios riguroso para controlar y Documentar todos los cambios en la infraestructura y los sistemas de AWS.

• Se realizan evaluaciones de riesgos y pruebas exhaustivas antes de Implementar cambios en producción para minimizar el impacto en la seguridad y la disponibilidad.

• Se mantiene un registro detallado de todos los cambios realizados y se proporciona transparencia a los clientes sobre los cambios que pueden afectar sus servicios.

Responsabilidades del Personal

• Todo el personal de AWS recibe capacitación en seguridad de la información y es responsable de cumplir con las políticas y procedimientos de seguridad.

• Se asignan roles y responsabilidades claras para garantizar una gestión efectiva de la seguridad en todos los niveles de la organización.

• Se establecen consecuencias claras para el incumplimiento de las políticas de seguridad, que pueden incluir medidas disciplinarias o legales según la gravedad de la infracción.

Conclusión:

La implementación de un manual de seguridad en un centro de procesamiento de datos es fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información crítica. Estas buenas prácticas proporcionan un marco estructurado y detallado que guía a los empleados y responsables en la protección de los activos de información contra amenazas internas y externas.

Además de establecer políticas y procedimientos claros, un manual de seguridad ayuda a promover una cultura de seguridad dentro de la organización al educar a los empleados sobre los riesgos de seguridad y las mejores prácticas para mitigarlos. Esto incluye aspectos como el manejo adecuado de contraseñas, la protección física de los equipos y la identificación de posibles vulnerabilidades en el sistema.

La existencia de un manual de seguridad también es esencial para cumplir con los requisitos regulatorios y legales relacionados con la protección de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea o la Ley de Privacidad del Consumidor de California (CCPA) en los Estados Unidos.

Es difícil nombrar una única empresa como la que tiene los mejores protocolos de seguridad en su centro de procesamiento de datos, ya que muchas organizaciones

líderes en el sector tecnológico invierten fuertemente en la seguridad de sus infraestructuras. Sin embargo, algunas de las empresas más conocidas por sus altos estándares de seguridad incluyen a Google, Amazon Web Services (AWS), Microsoft Azure e IBM.

Estas empresas implementan una amplia gama de medidas de seguridad, que incluyen controles físicos, como acceso restringido a sus centros de datos y sistemas de vigilancia avanzados, así como controles lógicos, como cifrado de datos, autenticación multifactor y detección y respuesta ante incidentes. Además, estas empresas suelen realizar auditorías de seguridad de forma regular y participar en programas de divulgación de vulnerabilidades para mejorar continuamente su postura de seguridad.

En última instancia, la eficacia de los protocolos de seguridad de un centro de procesamiento de datos depende de una combinación de medidas técnicas, procesos sólidos y una cultura organizacional centrada en la seguridad.

Referencias:
¿Qué es AWS Security Hub? - AWS Security Hub. (s. f.). https://docs.aws.amazon.com/es_es/securityhub/latest/userguide/what-is-securityhub.html

Protección de datos - Amazon Web Services (AWS). (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/compliance/data-privacy-faq/