SEGURIDAD EN LA NUBE

AUTOR: RICARDO CASTILLO B

NOVIEMBRE: 2020

San Marcos

Introducción

Aunque muchas personas entienden los beneficios del cloud computing, les da miedo implementarlo por las amenazas de seguridad. Es difícil comprender algo que se encuentra en algún lugar entre los recursos abstractos enviados por Internet y un servidor físico. Es un entorno dinámico donde todo cambia constantemente, incluso las amenazas de seguridad.

Contenido

Seguridad en la nube

¿Qué es la seguridad de TI: Cloud Security?

La seguridad en la nube es la protección de los datos, las aplicaciones y las infraestructuras involucradas en cloud computing. Muchos aspectos de la seguridad de los entornos de nube, ya sea pública, privada o híbrida, son los mismos que los de cualquier arquitectura de TI on-premise.

Las preocupaciones de seguridad de alto nivel (como la exposición de datos no autorizada o la filtración de información, los controles de acceso vulnerables, la susceptibilidad a los ataques y las interrupciones de la disponibilidad) afectan a la TI tradicional y a los sistemas de nube por igual. Al igual que en cualquier entorno informático, la seguridad en la nube implica mantener una protección preventiva adecuada que le permita lo siguiente:

- Estar al tanto de la seguridad de los datos y los sistemas.
- Ver el estado actual de la seguridad.
- Saber inmediatamente si sucede algo inusual.
- Hacer un seguimiento y responder ante eventos inesperados.

¿Por qué la seguridad en la nube es diferente?

Aunque muchas personas entienden los beneficios del cloud computing, les da miedo implementarlo por las amenazas de seguridad. Es difícil comprender algo que se encuentra en algún lugar entre los recursos abstractos enviados por Internet y un servidor físico. Es un entorno dinámico donde todo cambia constantemente, incluso las amenazas de seguridad. Una vez que entienda las diferencias específicas, la palabra "nube" no generará tanta inseguridad.

Seguridad de perímetros

La seguridad está muy relacionada con el acceso. Generalmente, los entornos tradicionales controlan el acceso mediante un modelo de seguridad de perímetro. Los entornos de nube se encuentran extremadamente conectados, lo que facilita el tráfico para omitir las defensas tradicionales del perímetro. Las interfaces de programación de aplicaciones (API) que no son seguras, la gestión deficiente de la identidad y las credenciales, los secuestros de cuentas y los infiltrados malintencionados pueden representar amenazas para el sistema y los datos. Para evitar el acceso no autorizado a la nube, se debe adoptar un enfoque centrado en los datos.

Ahora todo está en el software

La palabra "nube" hace referencia a los recursos alojados que llegan al usuario a través del software. Las infraestructuras de cloud computing, junto con todos los datos que se procesan, son dinámicas, escalables y portátiles. Los controles de seguridad en la nube deben responder ante las variables del entorno y acompañar las cargas de trabajo y los datos en reposo y en tránsito, ya sea como partes inherentes de las cargas de trabajo

(p. ej., cifrado) o de forma dinámica a través de un sistema de gestión de nube y API. Esto permite proteger los entornos de nube de la corrupción del sistema y la pérdida de datos.

Entorno de amenazas sofisticadas

Las amenazas sofisticadas constituyen todo aquello que impacta de forma negativa en la informática moderna que, sin duda, incluye a la nube. Los sistemas malware cada vez más sofisticados y los demás ataques, como las amenazas persistentes avanzadas (APT), están diseñados para evadir las defensas de la red aprovechando los puntos vulnerables de la pila informática. Las filtraciones de datos pueden dar lugar a la divulgación de información no autorizada y la alteración de los datos. No hay una solución clara para estas amenazas, pero es su responsabilidad estar al tanto de las prácticas de seguridad en la nube en constante evolución para mantenerse al día con las nuevas amenazas.

La seguridad en la nube es una responsabilidad de todos

Independientemente del tipo de implementación de nube que utilice, usted debe encargarse de la seguridad de su propio espacio en la nube. Usar una nube cuyo mantenimiento es responsabilidad de otra persona no significa que usted pueda, ni deba, relajarse. La falta de la diligencia correspondiente es la principal causa de las fallas en la seguridad. La seguridad en la nube es responsabilidad de todos, lo cual incluye tomar las siguientes medidas:

1. Usar software confiable
2. Entender el concepto de cumplimiento
3. Administrar los ciclos de vida
4. Considerar la portabilidad
5. Supervisar los entornos constantemente
6. Elegir al equipo de seguridad capacitado

¿Son seguras las nubes públicas?

Podríamos describir todas las diferencias de seguridad que existen entre los tres tipos de implementación (pública, privada e híbrida), pero sabemos que lo que en realidad la pregunta es si las nubes públicas son seguras.

Las nubes públicas son adecuadamente seguras para muchos tipos de cargas de trabajo, pero no son adecuadas para todo, en gran medida, porque no cuentan con el aislamiento de las nubes privadas. Las nubes públicas dan soporte a la arquitectura multiempresa, lo cual significa que usted alquila la potencia informática (o el espacio de almacenamiento) al proveedor de la nube junto con otras empresas. Cada inquilino firma un acuerdo de nivel de servicio (SLA) con el proveedor de la nube que documenta quién es responsable y por qué cosas se responsabiliza. Es muy parecido a alquilar un espacio físico a un arrendador. El arrendador (proveedor de la nube) promete realizar el mantenimiento del edificio (infraestructura de la nube), tener las llaves (acceso)

y, en general, no estorbar al inquilino (privacidad). A cambio, el inquilino promete no hacer nada (p. ej., ejecutar aplicaciones que no son seguras) que pudiera corromper la integridad del edificio o molestar a otros inquilinos. Pero usted no puede elegir a sus vecinos, y es posible que alguno de ellos permita el acceso a algo malicioso. Mientras el equipo de seguridad de infraestructura del proveedor de la nube controla si se producen eventos inusuales, las amenazas agresivas o imperceptibles (como los malintencionados ataques distribuidos de denegación de servicio [DDoS]) pueden afectar negativamente a otros inquilinos.

Afortunadamente, hay algunos estándares de seguridad, normativas y marcos de trabajo de control aceptados en el sector, como la matriz de controles en la nube de la Cloud Security Alliance. También puede aislarse en un entorno de arquitectura multiempresa implementando medidas de seguridad adicionales (como el cifrado y las técnicas de reducción de los DDoS), que protegen a las cargas de trabajo de una infraestructura comprometida. Si eso no es suficiente, puede lanzar agentes de seguridad de acceso a la nube para supervisar la actividad y aplicar las políticas de seguridad para las funciones empresariales de bajo riesgo. Sin embargo, es posible que todo esto no sea suficiente para los sectores que operan bajo normas de estricta privacidad, seguridad y conformidad.

Disminuir el riesgo con la nube híbrida

Las decisiones de seguridad están muy relacionadas con la tolerancia al riesgo y con el análisis de los costos y los beneficios. ¿Cuál es el impacto de los posibles riesgos y beneficios en el funcionamiento general de su empresa? ¿Qué es lo más importante? No todas las cargas de trabajo demandan el nivel más alto de cifrado y seguridad. Considérelo de esta manera: cerrar su casa con llave mantiene todas sus pertenencias relativamente seguras, pero, aun así, guarda sus cosas más valiosas en una caja fuerte. Es bueno tener opciones. Por eso cada vez más empresas adoptan las nubes híbridas, que ofrecen lo mejor de todas las nubes. La nube híbrida es una combinación de dos o más entornos interconectados de nubes públicas o privadas.

Conclusiones y recomendaciones

Las nubes híbridas le permiten elegir dónde colocar las cargas de trabajo y los datos en función del cumplimiento, las auditorías, las políticas o los requisitos de seguridad; de esta manera, protegen las cargas de trabajo especialmente confidenciales en una nube privada y ejecutan las cargas de trabajo menos confidenciales en la nube pública. Hay algunos desafíos singulares en cuanto a la seguridad en la nube híbrida (como la migración de datos, el aumento de la complejidad y una mayor superficie de ataque), pero la presencia de varios entornos puede constituir una de las defensas más fuertes contra los riesgos de seguridad.

Referencias bibliográficas

- RedHat. Seguridad en la nube. Qué es la segurdad de TI: Cloud Security? . Recuperado de https://www.redhat.com/es/topics/security/cloud-security

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica