arsys

6 pasos para mejorar la seguridad en el Cloud

La seguridad en el Cloud es algo indiscutible, pero no debemos dejar de lado estos seis pasos para mejorarla en lo posible.

La seguridad en el Cloud es un tema serio al que merece la pena atender en profundidad, de manera que no dejemos cabos sueltos y verifiquemos que, en estas cuestiones, la Nube cumple con los más estrictos estándares.

Aunque lo cierto es que las reticencias con la seguridad en el Cloud son cada vez menos frecuentes, a medida que aumenta la adopción de estas soluciones entre las empresas aumenta, en proporción, el número de ellas que tienen y plantean sus dudas. Como ya comentamos en alguna otra ocasión, las barreras para la adopción del Cloud son las mismas que hace unos años, aunque varían las razones.

Para eliminar cualquier posible duda que se pueda plantear, qué mejor que esta guía de seis pasos para mejorar la seguridad en el Cloud.

Disponer de herramientas de gestión de identidad y acceso

Controlar y gestionar adecuadamente quién tiene acceso a qué datos y servicios en la Nube debería ser lo más básico en cualquier política de seguridad. Sobre todo si hablamos de Cloud Público en el que los paneles de administración y las propias aplicaciones son accesibles para cualquiera que disponga de conexión a Internet.

Por eso, la base de cualquier estrategia para mantener el control es esa gestión de la identidad y el acceso. En este contexto, una de las mejores estrategias de seguridad en el Cloud es el **principio del mínimo privilegio**. Si además somos lo suficientemente ágiles como para solicitar y otorgar permisos (y revocar aquellos que ya no se necesitan), estaremos siendo muy eficientes, además de seguros.

Prevenir las malas configuraciones de seguridad

Como sucede en prácticamente cualquier aplicación o servicio online actual, la mayor amenaza para el Cloud son las **malas configuraciones** (junto con malas contraseñas o sistemas de acceso).

Los **errores de configuración en cualquier servicio en el Cloud** es una de las primeras cosas que va a comprobar un potencial atacante. Un desliz de seguridad aparentemente no muy importante, como podría ser el hecho de no eliminar una cuenta de usuario que ya no se utiliza, puede causar problemas en cualquier momento.

Entre las formas comunes en que una nube puede estar mal configurada se incluyen la **falta de restricciones de acceso y la falta de protección de datos**, en particular para la información personal que se sube en forma de texto plano en la nube.

Tampoco podemos olvidar a esos usuarios que disponen de excesivos permisos, es decir, permisos para servicios que no utilizan, o acceso con privilegios sobredimensionados por comodidad (en previsión de que, en un futuro cercano, los solicitarán). Estos usuarios son un objetivo muy atractivo, considerados por los ciberdelincuentes como una “puerta de entrada fácil” a nuestra organización.

Simplificar la gestión del Cloud

Proteger eficazmente un solo servicio ya es un gran desafío para las empresas y a medida que se añaden servicios nuevos el reto de blindar los datos crece. Como sabemos, es muy frecuente que las empresas tengan que gestionar una nube híbrida, por muchas razones. Eso conlleva una infraestructura compleja, lo que puede dar lugar a una serie de riesgos de seguridad.

Por tanto, **reducir en lo posible la complejidad en la gestión de la Nube es fundamental** para tenerlo todo bajo control, por ejemplo, minimizando a lo imprescindible el número de proveedores con el que trabajar.

Poner máxima atención en la detección y la respuesta ante amenazas

Prevenir es curar, y merece la pena invertir tiempo y recursos en monitorizar el tráfico y la actividad hacia el Cloud, de manera que sea sencillo comprobar si se están siguiendo las directrices del **Data Governance**, por ejemplo. Para ello, hay quien se lanza a contratar herramientas específicas, aunque es aconsejable, antes de invertir en cualquier solución, investigar primero las capacidades que ofrece nuestro futuro proveedor en cuanto a gestión de logs, informes y análisis.

Cifrado

Este punto se entiende por sí solo. El cifrado de datos es una de las herramientas de seguridad más potentes que las empresas pueden utilizar para proteger sus datos por si, de alguna manera, cayesen en las manos equivocadas.

La protección de datos se vuelve imprescindible porque los datos, por defecto, salen de las instalaciones de la empresa. **El cifrado de los datos en movimiento y «en reposo» es obligatorio.**

La formación es vital

La formación de los usuarios acerca de los riesgos de seguridad que existen y en los que pueden incurrir es vital. El Cloud es todavía un concepto nuevo en muchas empresas y para muchos empleados y directivos, por lo que la capacitación, y disponer de guías detalladas que describan todos los procedimientos, **debe ser una prioridad máxima.**

arsys

www.arsys.es

www.facebook.com/arsys.es

twitter.com/arsys

www.linkedin.com/company/arsys-internet/