arsys

Cómo garantizar la seguridad en entornos Multicloud

Multicloud presenta retos de seguridad muy particulares que se han de abordar con la mayor prioridad. Aquí damos claves para lograrlo.

Cuando hablamos de **entornos Multicloud** nos referimos a un enfoque particular en el planteamiento del Cloud en el que se combinan varios servicios, y cada uno de ellos puede pertenecer a un proveedor diferente, ya sea de Nube Pública o Nube Privada.

La diferencia con respecto al Cloud Híbrido es fundamental, puesto que este último se refiere a la combinación de Servidores Dedicados y públicos, como Servidores Cloud o, dicho de otra manera, a una integración de servicios de Nube Privada y Pública que se utiliza en algunas organizaciones para ofrecer diferentes tipos y niveles de servicios.

Hay que decir que, a pesar de que pueda parecer al contrario, optar por una **estrategia Multicloud** no conlleva mayores riesgos de seguridad que hacerlo por una estrategia de Nube Híbrida. Existen algunas consideraciones para tener en cuenta en el caso de querer **garantizar la seguridad del Multicloud**, que vamos a ver a continuación.

Autenticación y autorización

Asegurarse de que los usuarios, administradores, auditores y componentes del sistema legítimos tengan un acceso adecuado a las aplicaciones y servicios puede ser complejo.

En primer lugar, debemos encontrar un marco de trabajo que admita los diferentes modelos de autenticación y autorización de los diferentes proveedores del Cloud, y que sea independiente de todos ellos.

Las políticas definidas no deben depender de las aplicaciones, sino que deben estar diseñadas de acuerdo con nuestros propios requisitos de seguridad.

Actualización completa

Las cargas de trabajo deben estar utilizando la versión más reciente disponible de cualquier dependencia, middleware, o ejecutable. Esto puede significar actualizar o aplicar parches, reiniciar la carga de trabajo con la última imagen disponible o verificar y volver a cargar las dependencias recientes.

La razón de esto es que un entorno Multicloud es más heterogéneo por naturaleza que un entorno de Cloud Híbrido, y las vulnerabilidades y estrategias de mitigación correspondientes pueden variar de un proveedor a otro.

Asegurar la resiliencia

En un entorno Multicloud hemos de asegurarnos de que las aplicaciones estén protegidas contra los ataques y que sean resistentes a los compromisos de seguridad.

Para una aplicación que disponga de componentes en varias nubes, o para implementaciones con aplicaciones que se comunican entre sí a través de varias nubes, hacer un seguimiento de estas vulnerabilidades es más complejo que en los casos de entornos más estáticos.

Perfeccionar la monitorización

En un entorno menos complejo, confiamos en las herramientas de un único proveedor de servicios en el Cloud. En otros casos, podemos haber optado por una solución a medida de nuestra implementación en particular, pero en entornos Multicloud esto cambia drásticamente. No solo hablamos de más proveedores que son inherentemente independientes, sino que hemos de integrar nuestras herramientas de monitorización con cualquier herramienta disponible en un entorno más amplio.

Almacenamiento seguro

Puede parecer que la seguridad es un problema menor en comparación con el diseño de un sistema que permita el almacenamiento en diferentes Clouds, pero debe ser un requisito fundamental. El almacenamiento seguro siempre es una cuestión delicada, y lo es más en Multicloud. Por ello, mantener la compatibilidad es crítico y asegurar una administración de claves conveniente es fundamental para garantizar el éxito, y la seguridad.

Confidencialidad a través de varias Nubes

Cuando hablamos de **seguridad de los datos** nos referimos a datos en reposo (en el almacenamiento) y en tránsito (en la red). Sin embargo, existe un tercer estado de los datos que se vuelve importante en entornos Multicloud: en uso, cuando realmente se están procesando. Para los datos que son confidenciales debemos tener presente dónde se van a procesar y si ello es posible de acuerdo con nuestras políticas de confidencialidad.

El hecho de tener datos confidenciales moviéndose entre varias nubes hace que sea obligatorio controlar a la perfección esos itinerarios. En ocasiones, se debe prohibir ese tránsito por diversos motivos. Esto implica que deben desarrollarse nuevas tecnologías que protejan los datos mientras están en uso, algo que, de momento, está en proceso.

arsys

www.arsys.es

www.facebook.com/arsys.es

twitter.com/arsys

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