Multicloud: cómo reducir la superficie de exposición a los riesgos de ciberseguridad

Al utilizar múltiples nubes, una empresa multiplica de facto los puntos de acceso potenciales a sus aplicaciones para los piratas informáticos. Cifrado, parcheo, microsegmentación de redes… ¿Qué hay de las buenas prácticas para afrontar este reto?

Multi-nube: definición

La nube múltiple consiste en utilizar varios proveedores de nube . Las empresas utilizan esta estrategia a gran escala (casi 8 de cada 10 según un estudio de 451 Research) por varias razones: Optimizan sus costos; Son más ágiles; Evitan depender de un solo proveedor; Aprovechan lo mejor de cada entorno; Creen que están reduciendo los riesgos en caso de un ataque ciberdelincuente. La nube múltiple parece tener un futuro brillante: según un estudio publicado en julio pasado por IDC, el 85% de las organizaciones esperan adoptarlo en los próximos dos años.

Sin embargo, si las ventajas son innegables, también debemos considerar las múltiples nubes en el lado de las vulnerabilidades de seguridad. Sin embargo, esto presupone la adopción de un enfoque integral, cuidadosamente considerado en la fase inicial. Después de cambiar a la nube híbrida, la nube múltiple es el siguiente paso en el camino hacia el «cloud«. Al utilizar varios proveedores de nube, públicos o privados,

una empresa limita su riesgo de dependencia tecnológica. Puede seleccionar, proveedor por proveedor, los servicios más competitivos o más innovadores en un momento determinado.

Dos tercios de los tomadores de decisiones han adoptado una estrategia multi nube y su organización utiliza al menos dos plataformas de nube pública , según una encuesta de BPI Network.. Sin embargo, los beneficios reconocidos de la multinube se compensan con problemas de seguridad. Para el 63% de los profesionales de TI encuestados por BPI, la seguridad de las distintas nubes, pero también la de las redes, las aplicaciones y los flujos de datos, representan el principal desafío a cumplir.

Análisis

«En sí mismo, la multinube no crea más vulnerabilidades de las que ya existían, pero agrega complejidad a la complejidad existente», dijo Christophe Bardy, estratega de soluciones de Nutanix. «Una empresa que hasta ahora dependía de un sistema ciberseguro existente con sus propias limitaciones ahora debe comprender los diferentes ecosistemas. Hay tantas configuraciones multicloud como empresas».

Si bien los proveedores de nube pública promocionan sus características de seguridad, certificaciones y estándares de calidad, estos difieren de una nube a otra. Esto genera una inversión en tiempo y capacitación para el cliente con el fin de hacer malabarismos con varias interfaces de gestión y administración que permitan configurar mejor estos sistemas de seguridad propietarios. “Entre las configuraciones inadecuadas y el compromiso de los datos de autenticación, los riesgos son más específicos para cada cliente que para los jugadores de la nube”, agrega Geoffrey Portier, gerente regional de ventas de canales de Entrust. «Los proveedores han comercializado bien sus ofertas.

Es tan fácil suscribirse a servicios en la nube que a veces se

pasan por alto los problemas de seguridad». Mylène Jarossay, directora de seguridad de la información de LVMH y presidenta de Cesin (Club de seguridad de la información y expertos digitales), está de acuerdo. «Dominar la complejidad y escalabilidad de las nubes requiere una experiencia que aún no es tan común en el mercado. Si bien existen similitudes entre las grandes nubes públicas, es imperativo conocer los detalles técnicos de cada una y monitorear continuamente el desarrollo de sus diferentes módulos», ella argumenta. Entre proveedores y clientes, percibe «una sensación de desequilibrio permanente o la ausencia de una posible referencia».

Traiga su propia clave y cifrados

La reversibilidad, una de las promesas de la multinube, plantea, según Geoffrey Portier, otro problema de seguridad. «Cada proveedor tiene sus propios mecanismos de protección de datos, una empresa que desee transferir datos de un proveedor a otro primero tendrá que descifrar estos datos, garantizar esta transferencia de forma clara y luego utilizar otro cifrado «. Predicando por su parroquia, Geoffrey Portier aconseja configurar una solución BYOK (Traiga su propia clave) o BYOE (Traiga sus propias encriptaciones) que se integre con los dispositivos de seguridad de los proveedores de nube pública.

Un paso más allá, un HSM (módulo de seguridad de hardware) permitirá a una empresa generar, almacenar y proteger sus propias claves criptográficas. «Esto le permitirá mantener el control del proceso e interactuar con uno o más proveedores de servicios sin recurrir a sus soluciones de cifrado», explica Geoffrey Portier. Respecto a Nutanix, Christophe Bardy insiste en la importancia del parcheo. «Una máquina virtual básica es segura, pero una máquina virtual con un sistema operativo y una aplicación no lo es. Es necesario parchear el sistema operativo para llenar cualquier laguna. Sin embargo, muchas empresas son reacias a hacer este trabajo. Consume tiempo y es

un factor en la indisponibilidad de la plataforma ”, admite el experto. “Al mismo tiempo, también se trata de estandarizar los niveles de protección desde arriba y asegurar que los servicios en la nube cumplan con los estándares vigentes como PCI DSS para pagos en línea”. Christophe Bardy no olvida la dimensión de la red que involucra conexiones dedicadas como Direct Connect de AWS o ExpressRoute de Azure. “¿Qué hacer por encima de esta capa de transporte?”, Pregunta. Recomienda optar por una solución de microsegmentación de red. «Por ejemplo, permite aplicar una política de seguridad homogénea a una aplicación local con desbordamiento en la nube pública. Una empresa víctima de ransomware podrá recrear fácilmente su entorno».

Los peligros de la nube múltiple

Si bien los ejecutivos están entusiasmados, los CIO son mucho más reacios a utilizar la nube múltiple. Y con sobrada razón. Son plenamente conscientes de todo lo que hay detrás de esta gran oportunidad, especialmente en lo que respecta a la protección de datos personales. Por lo tanto, apenas son más de uno de cada dos (51%) para considerar embarcarse en la nube múltiple para 2021 (estudio de Markness). Para ellos, este enfoque es sobre todo sinónimo de «complejidad» por varias razones: Los riesgos de seguridad se multiplican; Puede haber problemas de interoperabilidad entre entornos; Como beneficio adicional, esto también implica dificultades de supervisión asociadas.

Respuestas técnicas y organizativas

Por su parte, Mylène Jarossay recuerda la importancia del control de acceso basado en roles o RBAC (control de acceso basado en roles). Un usuario medio utilizará una máquina virtual existente, pero no podrá crear una nueva o eliminar una a diferencia de un administrador o un superadministrador.

«Las delegaciones deben respetar los principios del mínimo privilegio y concederse en el perímetro más pequeño posible», recomienda Mylène Jarossay.

En cuanto a seguimiento, recomienda suscribirse a la opción de analizar los logs de proveedores que, aunque pagando en cuanto a almacenamiento y consultas, le parece imprescindible. Para Mylène Jarossay, los desfiles son técnicos pero también organizativos. En el campo de SaaS, se trata de luchar contra la TI en la sombra, un fenómeno que sigue, según ella, en constante aumento.

En cuanto a las aplicaciones Saas legítimas, es necesario «transferir su seguridad al editor asegurándose de que tiene la seguridad integrada adecuadamente 'por diseño' y que opera su plataforma de manera segura». Asimismo, los expertos en entornos de TI heredados deben revisar sus prácticas e integrar los nuevos criterios de confidencialidad, integridad, disponibilidad y trazabilidad en el mundo de la multicloud. Un proyecto a largo plazo.

Tendencia

Además, con el 81% de los usuarios trabajando con dos o más proveedores, el modelo multinube está en proceso de convertirse el nuevo estándar. Al aprovechar lo mejor de cada nube, ya sea en infraestructura, seguridad, disponibilidad, las empresas tienen la capacidad de lograr un modelo adecuado para sus datos y aplicaciones. Sin embargo, esta progresión plantea el tema de la gobernanza de este modelo, especialmente para organizaciones sujetas a estrictas regulaciones en los sectores bancario, salud, telecomunicaciones y público, por ejemplo.

Estos deberán establecer un marco de gobernanza para su primera nube y luego extenderlo a las siguientes nubes para garantizar la coherencia de los servicios utilizados en cada una de ellas con las aplicaciones compatibles. Más allá del

abanico de oportunidades que ofrece la nube múltiple, también permite limitar la dependencia de un proveedor. De hecho, según Gartner, las estrategias de múltiples nubes reducirán la dependencia de los proveedores para dos tercios de las organizaciones para 2024. Finalmente, este modelo ayuda a mejorar la continuidad del negocio de las organizaciones, especialmente en caso de falla o degradación del rendimiento de una de sus nubes. Al replicar sus datos e infraestructura en varios de ellos, minimizarán el riesgo de interrupciones.

Leer también: Data center, edge cloud, nube híbrida y atada ; Cloud backup y cloud storage, diferencias y similitudes ; Características de Veeam Cloud backup, para qué sirve, alternativas