Aumentan las filtraciones de datos en la nube

El 2022 Thales Cloud Security Report (Informe de seguridad en la nube 2022 de Thales), elaborado por 451 Research, que forma parte de S&P Global Market Intelligence, revela que el 45% de las empresas han sufrido una filtración de datos en la nube o no han podido superar una auditoría en los últimos 12 meses, lo que supone un aumento del 5% con respecto al año anterior, lo que aumenta la preocupación por la protección de los datos sensibles frente a los ciberdelincuentes.

A nivel mundial, la adopción de la nube, y en particular de la multinube, sigue aumentando. En 2021, las organizaciones de todo el mundo utilizaban una media de 110 aplicaciones de software como servicio (SaaS), frente a solo ocho en 2015, lo que demuestra un aumento sorprendentemente rápido. La utilización de múltiples proveedores de IaaS ha experimentado una notable expansión: el 72% de las empresas utilizan múltiples proveedores de IaaS, frente al 57% del año anterior. El uso de múltiples proveedores casi se ha duplicado en el último año, el 20% de los encuestados que declaran utilizar tres o más proveedores.

A pesar de una mayor prevalencia y uso, las empresas comparten preocupaciones respecto a la creciente complejidad de los servicios en la nube, ya que el 51% de los profesionales de TI coinciden en que es más complejo gestionar la privacidad y la protección de datos en la nube. Además, la transición a la nube también se está volviendo más compleja, ya que el porcentaje de encuestados que declaran que esperan «levantar y cambiar», la más sencilla de las tácticas de migración, ha descendido del 55% en 2021 al 24% en la actualidad.

Desafíos de seguridad ante la complejidad de la multinube

El aumento de la complejidad conlleva una necesidad mucho mayor de una ciberseguridad sólida. Cuando se les preguntó qué porcentaje de sus datos sensibles se almacenaban en la nube, el 66% respondió que entre el 21% y el 60%. Sin embargo, el 25% respondió que podía clasificar completamente todos los datos.

Asimismo, el 32% de los encuestados admitió haber tenido que emitir una notificación de filtración a una agencia gubernamental, cliente, socio o empleados. Esto debería ser motivo de preocupación para las empresas con datos sensibles, sobre todo en sectores muy regulados.

Los ciberataques también representan un riesgo constante para las aplicaciones y los datos en la nube. Las respuestas indican que la prevalencia de ataques es cada vez mayor: el 26% menciona un aumento de malware, el 25% de ransomware y el 19% afirma haber visto un aumento de phishing/whaling.

Proteger los datos sensibles

Si se trata de proteger los datos en entornos multinube, los profesionales de TI consideran que el cifrado es un control de seguridad fundamental. La mayoría de los encuestados citaron el cifrado (59%) y la gestión de claves (52%) como las tecnologías de seguridad que utilizan actualmente para

proteger los datos sensibles en la nube.

Sin embargo, cuando se les preguntó qué porcentaje de sus datos en la nube estaba cifrado, solo el 11% de los encuestados declaró que entre el 81% y el 100% estaba cifrado. Además, la proliferación de plataformas de gestión de claves puede ser un problema para las empresas. Solo el 10% de los encuestados utiliza una o dos plataformas, el 90% utiliza tres o más, y el 17% admitió utilizar ocho o más plataformas.

El cifrado debería ser un área prioritaria para las empresas a la hora de proteger los datos en la nube. De hecho, el 40% de los encuestados declaró que pudo evitar el proceso de notificación de filtraciones porque los datos robados o filtrados estaban cifrados o tokenizados, lo que demuestra el valor tangible de las plataformas de cifrado.

Además, resulta alentador comprobar que las empresas adoptan el principio Zero Trust e invierten en consecuencia. El 29% de los encuestados afirmó que ya está ejecutando una estrategia de Zero Trust, el 27% dijo que está evaluando y planificando una, e incluso el 23% señaló que la está considerando. Se trata de un resultado positivo, pero sin duda todavía queda margen de crecimiento.

Sebastien Cano, **vicepresidente sénior de Actividades de Protección de la Nube y Licencias de Thales,** ***comentó:*** *«La complejidad de la gestión de los entornos multinube no se puede sobrevalorar. Además, la creciente importancia de la soberanía de los datos está planteando cada vez más preguntas a los directores de seguridad de la información y a los responsables de la protección de datos a la hora de considerar su estrategia, gobierno y gestión de riesgos en la nube. No se trata únicamente de dónde residen geográficamente los datos sensibles, sino incluso de quién tiene acceso a ellos dentro de la organización.*

Las soluciones son diversas, como el cifrado y la gestión de claves. Por último, pero no por ello menos importante, seguir adoptando una estrategia de Zero Trust será esencial para asegurar estos complejos entornos, ya que ayudará a garantizar que las organizaciones puedan respaldar sus datos y gestionar los retos futuros».

Thales y 451 Research comentarán los resultados con más detalle durante un seminario web el 23 de junio de 2022. Para participar, visite la página de inscripción.