Las empresas luchan contra la inseguridad de la nube con identidades no personales

La **explosión de identidades no humanas en las implementaciones de la nube pública hace que los responsables de la toma de decisiones recurran a nuevas herramientas de gestión de acceso e identidad** para mantener sus entornos seguros. Así lo confirma un nuevo estudio realizado por Forrester.

El estudio fue publicado bajo el título 'Los controles de identidad son fundamentales para los planes empresariales de seguridad en la nube'. Este encontró que más de la mitad de los 154 tomadores de decisiones de seguridad y TI de América del Norte encuestados para el informe reconocieron que **estaban luchando con identidades de máquinas y no personas que proliferan en la nube.**

Lo que muchas organizaciones que se han mudado a la nube están descubriendo es que están pensando mucho **en las identidades de las personas, pero no están pensando en las identidades que no son personas, que suponen magnitudes mayores que las identidades de personas. Es un verdadero punto ciego para las organizaciones.** No ven los riesgos que las identidades representan para su nube.

Desafíos relacionados con los sistemas CIG/CIEM

Para abordar sus problemas de identidad en la nube, más de la mitad de los responsables de la toma de decisiones (55 %) afirmó que sus organizaciones están invirtiendo en soluciones de gobierno de la identidad en la nube **(CIG)** y gestión de derechos de infraestructura en la nube **(CIEM)** y, para 2023, el **82%** hará lo mismo. A pesar de la voluntad de invertir en **CIG/CIEM,** el estudio encontró que casi todos **(98%)** enfrentan desafíos de seguridad relacionados con los sistemas.

Esos desafíos incluyen: políticas de control de acceso demasiado complejas que hacen que configurar menos privilegios entre las identidades de la nube sea casi imposible de lograr; herramientas heredadas que no pueden integrarse bien, o en absoluto, en el entorno de la nube pública y que permiten la persistencia de identidades de corta duración y la proliferación de identidades de máquinas y no personas no reconocidas; y, por último, dificultades para ver una vista única de las identidades de la plataforma en la nube.

Investigación impulsada por IA

Los investigadores de Forrester también descubrieron que las soluciones impulsadas por **IA** se han convertido en una prioridad para las organizaciones que participan en la encuesta. La mitad de los encuestados señaló que los programas de investigación o detección de comportamiento impulsados por la **IA** eran objetivos principales para sus programas de seguridad en la nube. Dada la escala y la velocidad de la nube, la **IA** tiene que estar allí. Las cosas deben hacerse mucho más rápido de lo que se puede hacer con un script o un programa simple. La nube debe protegerse a la escala y la velocidad de la misma.

A medida que las organizaciones continúan aumentando su uso de la nube pública, se enfrentan a mayores desafíos para administrar la seguridad de sus instancias en la nube, incluida la aplicación de las configuraciones y ajustes correctos a escala, señaló el informe. Con el creciente número de servicios, roles y políticas en la nube escritos en código, existe un crecimiento exponencial en los posibles controles de permisos. Para satisfacer mejor estas necesidades, siguió, las organizaciones buscan soluciones **CIG/-CIEM,** monitoreo e investigación impulsados por la **IA** y una mejor automatización de los flujos de trabajo manuales que consumen mucho tiempo para la investigación, las revisiones de acceso y la reparación.

Fuente de información: cio.com.mx