Articulos

¿Le tiene miedo a la nube? Recomendaciones de seguridad para ver a los fantasmas

Por Juan Carlos Zevallos | Gerente de IBM Security para Latinoamérica

October 30, 2023

Las empresas emprenden su viaje tecnológico a la nube híbrida por las razones correctas: para lograr dinamismo, diversificación, innovación, flexibilidad y velocidad en su negocio. Por eso, hoy 99% de las empresas a Argentina[1] la usa, convirtiendo a la nube hibrida en la arquitectura tecnológica dominante. Con múltiples herramientas, servicios y nubes de varios proveedores, podría decirse que las empresas tienen un “Frankenstein” tecnológico. Y en esa complejidad está el desafío de seguridad.

Según el IBM X-Force 2023 Cloud Threat Landscape Report, el equipo de X-Force rastreó casi 3.900 vulnerabilidades relacionadas con la nube, una cantidad que se duplicó desde 2019. El reporte también reveló que, aunque los cibercriminales buscan constantemente mejorar su productividad, no se apoyan exclusivamente en la sofisticación para lograrlo. Siguen utilizando tácticas simples pero confiables que ofrecen facilidad de uso y, a menudo, acceso directo a entornos privilegiados.

Los atacantes continúan tejiendo redes de araña para obtener credenciales legítimas de acceso (usuarios y contraseñas) e ingresar a las organizaciones. De hecho, el uso inadecuado de credenciales con permisos excesivos fue la principal causa de los incidentes de seguridad en la nube a los que X-Force respondió en el mundo. Cuando la nube hace parte de la superficie de ataque, las credenciales comprometidas podrían usarse incluso para acceder a las tecnologías sin generar niveles apropiados de sospecha o detección.

Considerando que en la región, 43% de las filtraciones de datos en la nube híbrida resultan en pérdida de datos, estas son tres recomendaciones para que las empresas identifiquen sus brechas en la nube:

Repensar los controles de identidad y acceso

Es clave contar con controles suficientes para garantizar que "los usuarios sean quienes dicen ser". Modernizar la gestión de accesos (IAM), fortalecer las políticas y prácticas de control de acceso, establecer principios de privilegios mínimos y aumentar las exigencias de autenticación multifactor para cuentas privilegiadas es un gran paso. Las capacidades de IA también ayudan a examinar las identidades digitales, detectar

comportamientos anormales y verificar la legitimidad de los usuarios.

Conocer su superficie de ataque

Como no se sabe lo que no se conoce, las organizaciones tienden a estar más expuestas de lo que se dan cuenta. Gestionar la superficie de ataque es una forma de comprender la suma de vulnerabilidades, rutas o métodos que los cibercriminales pueden usar para obtener acceso no autorizado a las organizaciones para llevar a cabo un ciberataque. Es la manera de descubrir la extensión total de la tecnología de una empresa en la sombra para ver a los fantasmas.

Poner a prueba la postura de seguridad

Simular ataques utilizando escenarios basados en la nube es un buen ejercicio para entrenar y practicar una respuesta efectiva ante los incidentes. Esto debe ir de la mano de las pruebas de penetración para encontrar y corregir las fallas que puedan exponer la nube a los atacantes. Las pruebas manuales pueden ayudar a descubrir fallas que las herramientas por sí solas no pueden encontrar, como configuraciones incorrectas o privilegios excesivos.

Tal vez, la pregunta que muchos pueden hacerse es: ¿por qué los cibercriminales eligen atacar la nube? Las razones pueden variar; sin embargo, algunas incluyen la minería de criptomonedas. Por ejemplo, quienes están detrás de la criptominería ven en la nube los recursos para la minería que de otra manera serían muy costosos, trasladando el costo a las empresas. Además, si la nube recibe un monitoreo menos exhaustivo, el malware puede funcionar durante más tiempo antes de ser detectado y eliminado.

Y todo comienza principalmente con las credenciales legítimas que están comprometidas, que son la máquina de dinero de la dark web y se venden por tan sólo US 10. Es claro que este es un vector de amenaza "activo" y que es imprescindible que las organizaciones puedan abordarlo. Por eso, conocer de antemano la ruta y el posible destino de los cibercriminales pueden evitar muchos dolores de cabeza. “Quien piense que no es atacado, no está buscando lo suficiente”.

---

[1] *IBM & Oxford Economic: Cloud’s next leap*

Article Categories