Seguridad en la nube: qué necesitas saber

Casi todas las empresas se están pasando a la nube, ya sea siguiendo una acción planificada o motivadas por la utilización por parte de sus empleados de servicios de nube no autorizados. Los empleados suelen recurrir a los servicios en la nube para ser más eficientes, pero no tienen en cuenta las implicaciones en materia de seguridad, un verdadero quebradero de cabeza para los directivos de la empresa.

Por desgracia, las empresas a menudo se centran en temas equivocados en lo referente a la seguridad en la nube. Los proveedores de servicios de nube, por lo general, hacen un buen trabajo a la hora de protegerse (mejor que las empresas). Por eso, no deberías preocuparte en exceso en lo referente a la seguridad de sus servicios ni temer que puedan ser hackeados.

> La amenaza más preocupante para la infraestructura de nube son las intrusiones, que pueden obedecer a una amplia variedad de causas.

De hecho, deberías preocuparte de las partes de la nube que controlas. Dichas preocupaciones variarán en función del tipo de nube que tu empresa contrate. La opción de infraestructura como servicio (IaaS) te ofrece mayor control sobre la seguridad pero también conlleva una mayor responsabilidad. Por su parte, el software como servicio (SaaS) te ofrece un menor control sobre la seguridad y transfiere la responsabilidad a tu proveedor de servicios. La plataforma como servicio (PaaS) es una mezcla de ambas opciones.

Por estas razones, el modelo de servicios de nube que adoptes determinará el nivel de responsabilidad de tu proveedor en materia de seguridad. Esto es lo que necesitas saber.

1. Comprender las amenazas a las aplicaciones y la infraestructura de nube

La amenaza más preocupante para la infraestructura en la nube es la misma que con cualquier otra infraestructura: la intrusión, que podría tener una amplia variedad de causas. Es importante reconocer que existen distintos niveles de intrusión; un atacante que acceda a una cuenta de administrador logrará un control mucho mayor que el que acceda a la cuenta limitada de un usuario.

Por esta razón, deberías preocuparte más de los usuarios con privilegios de usuario extensos o administrativos, y vigilar esas cuentas por encima de lo normal. Esta amenaza a la seguridad se aplica a todos los tipos de nube, dado que los empleados de la empresa mantienen algún tipo de acceso administrativo para los tipos de infraestructura SaaS, PaaS e IaaS.

2. Gestionar la identidad y el acceso de forma segura

Por extensión, deberías prestar atención especial a todo lo relativo a la identidad y el acceso con objeto de incrementar la seguridad de tus servicios de nube. El almacenamiento de datos de acceso e identidad debería estar protegido y ser vigilado de cerca. No obstante, dado que la mayoría de empresas deben lidiar de media con unas 1.031 aplicaciones en la nube, que son las que usan sus empleados, es algo que no puede lograrse sin disponer de un sistema federado de gestión de la identidad o una infraestructura única de gestión del inicio de sesión.

3. Compensar las amenazas con disponibilidad

Los ataques de denegación de servicio (DDoS) se han vuelto más sofisticados y fáciles de lanzar. Los servicios de alquiler de ataques DDoS, también llamados booters o stressers, están listos para atacar

redes o páginas web. Y dado que los servicios de nube se están volviendo más populares, los ataques DDoS tienen cada vez más impacto, haciendo que los atacantes puedan interrumpir servicios vitales de la empresa lanzando solo un ataque.

En octubre de 2016, por ejemplo, un gran ataque DDoS perpetrado por miles y miles de grabadoras de vídeo, cámaras y routers domésticos atacó el proveedor de DNS Dyn, cuyos clientes contrataban sus servicios para dirigir a los usuarios a sus páginas web. Como consecuencia, muchos servicios de Internet, entre los que estaban Netflix, Twitter y PayPal, dejaron de estar disponibles.

Necesitarás determinar si tu proveedor es lo suficientemente elástico como para soportar un ataque. Aunque muchos proveedores de infraestructura de nube ofrecen capacidades para aumentar el ancho de banda, a menudo cobran una cantidad añadida por dicho ancho de banda adicional utilizado durante un ataque, lo que puede resultar excesivamente caro para tu empresa. Tendrás que evaluar hasta qué punto te cuesta demasiado hacer frente al ataque y si tiene más sentido que contrates un servicio de mitigación de ataques DDoS que intercepte el tráfico malo antes de que acceda a tus aplicaciones.

4. Gestionar las amenazas de las vulnerabilidades

En 2015, un hacker usó una vulnerabilidad en la nube pública de la empresa de antivirus BitDefender para robar un número desconocido de nombres de usuario y contraseñas sin cifrar. Las vulnerabilidades no son una amenaza menor a la infraestructura de nube, sino que están al mismo nivel que las que pudiera haber en los dispositivos y herramientas de los equipos físicos de tu empresa.

Las empresas deben ser capaces de instalar parches de forma ágil, lo que significa que los equipos de operaciones necesitan saber qué componentes de la infraestructura son vulnerables y contar con opciones para gestionar dicha vulnerabilidad. El parcheado rápido debería ser una prioridad, pero la posibilidad de instalar parches virtuales también debería existir a fin de dar a los equipos de seguridad tiempo suficiente para reparar los problemas sin causar más incidencias.

Por lo general, los servicios y plataformas en la nube tienden a ser más seguros que la infraestructura media de las empresas dados los acuerdos de nivel de servicio, parcheado y actualizaciones regulares con los que cuentan. En consecuencia, las empresas deberían centrarse en los aspectos de la nube que están bajo su control. Las empresas descubrirán que la nube es una opción mucho más segura si se centran en controlar el acceso y las credenciales, en mantener los servicios disponibles y en gestionar las vulnerabilidades en aquellos aspectos de la infraestructura en la nube que están bajo su control.