Libro electrónico

Cinco desafíos de la seguridad de la nube que su empresa puede enfrentar de forma directa

rackspace technology | Microsoft Azure

La evolución constante de las amenazas cibernéticas y la carrera por tener herramientas más sofisticadas para combatirlas han generado un cambio rápido en el panorama de la seguridad. Ahora más que nunca, es importante comprender sus vulnerabilidades y reunir las soluciones adecuadas para fortalecer y proteger sus ambientes. Y la mejor manera de hacerlo es a través de la implementación de un programa de seguridad de vanguardia centrado en la mejora continua y respaldado por una gran experiencia.

En este libro electrónico, analizamos cinco desafíos de la seguridad que enfrentan las empresas y cómo los proveedores deben estar a la altura de las circunstancias para defenderlas.

1. No existe una solución de seguridad única.

Muchas veces, las empresas que se someten a proyectos de transformación digital se topan con problemas para trasladar sus controles, políticas y prácticas de seguridad existentes de un ambiente a otro. Trasladar las cargas de trabajo y tecnologías de seguridad existentes a la nube. La mayoría de las organizaciones aprovechan múltiples plataformas en la nube, y todas estas plataformas tienen su propia cartera de herramientas de seguridad nativas de la nube que, por lo general, no se integran con otras plataformas. Saber cómo diseñar sus ambientes multi-cloud para satisfacer sus necesidades de seguridad y compliance con la tecnología de seguridad adecuada es un desafío. La flexibilidad de las herramientas de seguridad que elija es importante a medida que cambian las necesidades de su negocio y las amenazas de ciberseguridad aumentan en complejidad. Las soluciones de seguridad deben ser rápidas, flexibles y elásticas.

Y lo más importante, las medidas de seguridad deben ser apropiadas para la nube. Es importante recordar que trasladar sus cargas de trabajo a la nube abre nuevos factores de riesgo, y se pueden implementar nuevas herramientas de seguridad para proteger sus aplicaciones y datos. Un estudio reciente de IDC reveló que el 79 % de las empresas había experimentado al menos un ataque en los últimos 18 meses. ¿Uno de los problemas persistentes para las organizaciones? La falta de visibilidad de los ambientes de nube en vivo, según los directores de seguridad de la información encuestados *(Encuesta de IDC a 200 encargados de tomar las decisiones de seguridad, 2020).*

Independientemente de dónde se encuentre en su recorrido hacia la transformación digital y el traslado de las cargas de trabajo a la nube, tenga en cuenta que podría necesitar diferentes herramientas de seguridad, políticas y planes de respuesta.

rackspace technology. | Microsoft Azure

2. Las aplicaciones son esenciales para la arquitectura moderna de la nube, pero no darle prioridad a la seguridad desde un principio puede generar grandes obstáculos.

Al igual que la nube, las amenazas actuales son dinámicas. La nube se centra en las aplicaciones, no en la infraestructura. Programadores, ingenieros de confiabilidad del sitio, propietarios de líneas de negocios y administradores de aplicaciones digitales la diseñan y ejecutan, y no los equipos de infraestructura de red tradicionales. Este es un cambio con respecto a los modelos de control que presentan un ritmo más pausado a los que están acostumbradas muchas empresas. Ahora que actuamos rápido, hay más automatización, velocidad y agilidad. La seguridad también necesita ser más ágil y adaptable. Los ingenieros de DevSecOps pueden ayudar a integrar la seguridad en el desarrollo de sus aplicaciones nativas de la nube desde el principio, sin ralentizar la velocidad de desarrollo.

¿Por qué? Dado que la nube se centra en las aplicaciones, esto genera un nuevo aumento de las amenazas que se centran en las aplicaciones.

Las amenazas a las aplicaciones están en auge: Según una encuesta reciente de Forrester, el 33 % de los ataques proviene de ataques externos, como ataques a aplicaciones web, credenciales robadas y ataques de explotación de software *(Encuesta sobre seguridad de Forrester Analytics Global Business Technographics® 2019)*.

Los errores de configuración de la nube dan lugar a ataques: Según Gartner, el 99 % de las fallas de seguridad de la nube será culpa del cliente *(Informe de seguridad de Gartner: Tendencias 2025)*.

3. La escasez de talento de hoy en día es un gran desafío para la industria de la seguridad.

Según el New York Times, hay una tremenda escasez de competencias. Se estima que a fines de 2021 habrá 3.5 millones de puestos de ciberseguridad sin cubrir. La mayoría de las empresas no tienen la experiencia ni las capacidades necesarias porque su personal carece de capacitación o experiencia en seguridad para proteger de forma adecuada sus ambientes en la nube y en las instalaciones. Sin expertos en seguridad en la nube con experiencia en la plantilla, las organizaciones tendrán dificultades para migrar a la nube de forma segura y transformar sus modelos operativos. Según Forrester, el 43 % de las organizaciones cita que la competencia por el talento en seguridad dificulta la contratación y retención de personal *(Encuesta sobre seguridad de Forrester Analytics Global Business Technographics® 2019)*. La fuerte competencia por el talento de seguridad y los exigentes mandatos de compliance han hecho que muchas empresas inviertan en servicios, en lugar de invertir en personal de seguridad más costoso y difícil de reclutar.

4. Una política de seguridad reactiva no es suficiente con el aumento del ransomware.

Cuando se trata de violaciones de seguridad, no es cuestión de ver si se producirá una, sino de saber cuándo sucederá. Una sola violación de seguridad puede devastar financieramente su organización, paralizar el trabajo y dañar su reputación. Muchos equipos de TI se esfuerzan por evitar quedar atrapados en un ciclo continuo de "modo reactivo", lo que limita su capacidad de mirar hacia el futuro de manera proactiva. Esperar hasta después de haberse visto afectado por un incidente de seguridad será más costoso a largo plazo y, probablemente, aumentará su exposición a nuevos incidentes en el futuro. De hecho, en el último año, el costo medio de una violación ha aumentado de US$3.9 millones a U$S4.24 millones en todo el mundo *(Ponemon, Costo de una violación de datos, 2021)*.

Aunque su empresa tenga implementado un plan de respuesta a incidentes de seguridad reactivo, aún podría estar en riesgo. Los ciberdelincuentes pueden pasar desde el acceso inicial hasta el secuestro de toda una red en menos de 45 minutos. *(Informe de Defensa Digital de Microsoft, septiembre de 2020)*. Esto puede suceder incluso cuando el ataque provoque múltiples alertas de detección en las herramientas de seguridad, como los productos de detección y respuesta de puntos de conexión, lo que significa que los ciberdelincuentes comprenden los desafíos que enfrentan los Departamentos de TI modernos en su incapacidad para clasificar, contener y responder de golpe a los rápidos atacantes.

rackspace technology | Microsoft Azure

5. La seguridad debe seguir el ritmo de su infraestructura.

Las nuevas amenazas evolucionan todo el tiempo, y muchas empresas se esfuerzan por mantenerse al día de las amenazas y vulnerabilidades que surgen a diario. Las nuevas técnicas de ataque son sofisticadas y combinan técnicas superpuestas para penetrar en un sistema, como el reconocimiento, la recolección de credenciales, el malware y los ataques por explotación de VPN, por nombrar solo algunas. Por si fuera poco, los actores maliciosos avanzados están desarrollando malware único, además de código malicioso disponible abiertamente para la actividad delictiva en línea dominante *(Informe de Defensa Digital de Microsoft, ejercicio fiscal 2020)*. Los enfoques tradicionales con respecto a la postura de seguridad no se adaptan a los modelos de entrega de aplicaciones que dan prioridad a la nube. La ventaja de una nube como Azure es la flexibilidad que proporciona para cambiar y satisfacer las necesidades de su empresa. Aunque es importante contar con un socio de seguridad que entienda la nube y esté dispuesto a comprometerse y seguir el ritmo, a medida que crecen sus necesidades, es aún más importante que lo ayude a hacer evolucionar sus operaciones de seguridad.

Cómo puede ayudar Rackspace Technology

Rackspace Elastic Engineering for Security lo ayuda a liberarse de los enfoques reactivos tradicionales de la seguridad con una solución de seguridad ágil, proactiva e integral que ofrece una detección eficaz de amenazas y respuesta ante incidentes contra ataques cada vez más sofisticados.

Impulsados por una estructura de pods que funciona como una extensión de su personal, lo ayudamos a cumplir con los objetivos de seguridad y compliance de la nube que son importantes para su empresa. No importa dónde se encuentre en su recorrido hacia la seguridad en la nube, su pod de expertos estará con usted en cada paso del camino, ayudando a su empresa a definir e implementar una estrategia de seguridad que reduzca el riesgo y defienda contra las ciberamenazas. Como su socio de seguridad, Rackspace Technology consolida la inteligencia de amenazas, el análisis de seguridad, las alertas y los servicios de respuesta en una solución que se puede implementar y administrar fácilmente en todos los ambientes multi-cloud.

Su pod incluye un gerente de contrataciones, un líder del pod, un arquitecto principal, arquitectos en seguridad, ingenieros en seguridad, un experto en compliance y analistas de seguridad/evaluadores de penetración que trabajan como una extensión de su equipo y se dedican a resolver los riesgos cibernéticos. Su pod de seguridad puede diseñar, construir y gestionar completamente una arquitectura de defensa total para alcanzar una protección unificada en todos los ambientes multi-cloud.

Como socio Gold de Microsoft, puede confiar en Rackspace Technology para que trabaje con usted, a fin de que pueda aprovechar las soluciones de Azure que abordan sus desafíos comerciales con respecto a las aplicaciones y la infraestructura, y que, al mismo tiempo, lo ayudan a generar nuevos flujos de ingresos y a aumentar la eficiencia.

Nuestros expertos en seguridad tienen un profundo conocimiento y experiencia, tanto en seguridad de TI como en la nube, y cuentan con más de 800 certificaciones de la industria de la seguridad, lo que incluye ingenieros en seguridad de Azure certificados por Microsoft.

Seguimos dedicándonos a ayudarlo a proteger sus inversiones digitales, mientras ayudamos a garantizar la resiliencia de la seguridad y a abordar sus necesidades de compliance. Somos su socio, y estamos listos para hacer posible resultados comerciales más predecibles y beneficios de transformación de la suscripción.

Obtenga más información en: www.rackspace.com/security/elastic-engineering o llame al 1-800-961-2888

Acerca de Rackspace Technology

Rackspace Technology es un experto en soluciones de nube múltiple. Combinamos nuestra experiencia con las tecnologías líderes del mundo, en aplicaciones, datos y seguridad, para ofrecer soluciones integrales. Contamos con una trayectoria comprobada de asesoramiento a clientes según sus desafíos comerciales, de diseño de soluciones que se escalan, de desarrollo y administración de esas soluciones y de optimización de beneficios para el futuro.

Como pioneros en los servicios de tecnología multi-cloud a nivel mundial, ofrecemos capacidades innovadoras de la nube para ayudar a los clientes a desarrollar nuevas fuentes de ingresos, aumentar la eficacia y crear experiencias increíbles. Con el prestigio de ser reconocidos como el mejor lugar para trabajar año tras año, según Fortune, Forbes y Glassdoor, atraemos y desarrollamos talentos de clase mundial para ofrecer la mejor experiencia a nuestros clientes. Todo lo que hacemos está impregnado de nuestra obsesión por el éxito de nuestros clientes —nuestra Fanatical Experience™— para que puedan trabajar más rápido, de manera más inteligente y anticiparse a lo que viene.

Obtenga más información en www.rackspace.com o llame al 1-800-961-2888.