El cloud computing puede respaldar sus funciones de seguridad de seis formas diferentes

La adopción del cloud computing lleva a que las empresas deban optar entre la rentabilidad, la capacidad de ajuste y la conveniencia de utilizar un entorno de nube, o la comodidad de mantener los datos y las aplicaciones alojados de forma segura en sus propios servidores. La pregunta que debemos hacernos es si el alojamiento en las instalaciones es realmente más seguro que en el cloud computing. Muchos especialistas opinan que no es así. A continuación, analizaremos seis factores que lo harán sentirse a gusto al optar por el cloud computing.

1 Los altos costos de la seguridad

Puesto que la seguridad requiere una inversión, debe preguntarse cuánto puede gastar en ella. Los costos de implementarla para los centros de datos en las instalaciones son demasiado elevados, especialmente para las pequeñas y medianas empresas. Por lo tanto, es poco factible lograr el nivel de protección que ofrecen los proveedores principales a los clientes.

2 La seguridad requiere contar con vasto personal

Se necesitan muchas personas para llevar a cabo esta actividad. Por ello, los proveedores de servicios de nube de gran envergadura disponen de equipos de protección que trabajan de forma permanente y de un centro de operaciones de seguridad completo en el que se supervisa la infraestructura de TI y el hardware físico constantemente. Microsoft Azure, por ejemplo, tiene más de 3500 especialistas en ciberseguridad para su protección. Pero la mayoría de las empresas no cuenta con el personal suficiente para brindar el mismo nivel de seguridad que los proveedores principales.

3 Los proveedores de servicios de nube están interiorizados en el ámbito de la seguridad

A usted le preocupa la seguridad, pero encargarse de ella es un tema más entre tantos otros. Sin embargo, para los proveedores de servicios de nube es una de las prioridades. Ellos deben ofrecer a sus clientes el mayor nivel de seguridad posible para continuar operando y compitiendo en el mercado. Por ejemplo, Google Cloud ofrece una infraestructura segura desde el diseño con protección integrada y cifrado predeterminado[1].

Microsoft Azure ayuda a identificar las amenazas "analizando orígenes enormes que incluyen 18 000 millones de páginas web de Bing, 400 000 millones de correos electrónicos, 1000 millones de actualizaciones de dispositivos Windows y 450 000 millones de autenticaciones cada mes. Con el uso de aprendizaje automático, análisis del comportamiento e inteligencia basada en aplicaciones, los científicos de datos de Microsoft analizan el flujo de datos en Microsoft Intelligent Security Graph"[2].

Los proveedores de servicios de nube también deben cumplir con los más altos estándares, como, por ejemplo, las certificaciones de terceros reconocidas en todo el mundo y las auditorías del personal, los procesos y las tecnologías de seguridad que se realizan mediante diversos programas rigurosos. Amazon Web Services (AWS), por ejemplo, suele obtener la validación de otros organismos en cuanto a miles de requisitos internacionales de cumplimiento. La mayoría de las empresas no dispone del tiempo, los recursos ni el presupuesto necesarios para lograr este nivel de garantía de seguridad[3].

1 *"Confianza y seguridad". Google. Se consultó el 29 de abril de 2022.*

2 *"Refuerce su seguridad con Azure". Azure. Se consultó el 29 de abril de 2022.*

3 *"AWS cloud security". Amazon. Se consultó el 29 de abril de 2022.*

4 Las herramientas avanzadas de seguridad

Los proveedores de servicios de nube implementan una amplia variedad de herramientas avanzadas de seguridad para proteger las aplicaciones y los datos de los clientes. AWS brinda controles detallados de acceso e identidades, supervisión permanente, detección de amenazas, protección para las redes y las aplicaciones, funciones automatizadas de respuesta y recuperación ante incidentes, múltiples capas de cifrado y mucho más. Los proveedores principales ofrecen acceso a cientos de soluciones adicionales de seguridad en las tiendas de sus partners. Es prácticamente imposible replicar este amplio conjunto de herramientas avanzadas en su red y su centro de datos. Los costos, el personal, el tiempo y el esfuerzo que requeriría hacerlo implican un gran compromiso para una empresa que no se especializa en seguridad.

5 La segmentación de las redes

Una ventaja de seguridad propia de los entornos de nube es la segmentación de las estaciones de trabajo de los usuarios. Los malhechores cibernéticos suelen atacar a usuarios específicos en el sistema a través de correos electrónicos y sitios web. En esos casos, ingresan a la red a través de las estaciones de trabajo de dichos usuarios.

Sin embargo, en un entorno de nube, estas estaciones solo disponen de la conectividad suficiente para que los usuarios realicen su trabajo y no cuentan con acceso directo a la red empresarial. Por lo tanto, aun si alguna de ellas se viera comprometida, el atacante no obtendría acceso a la empresa ni a sus aplicaciones y datos.

6 La seguridad física

La seguridad física sigue siendo un factor fundamental. Las personas con acceso físico directo al hardware pueden representar un riesgo grave para la seguridad. En cambio, si los datos y las aplicaciones se encuentran en un entorno de nube, ni los empleados descontentos ni aquellos que al trabajar en las instalaciones, sin intención, pudieran ocasionar daños, podrán acceder a estos recursos con facilidad. Es mucho más difícil que encuentren los datos en este tipo de entorno.

Además, los proveedores principales tienen los recursos para evitar el robo físico de datos, como guardias de seguridad, gabinetes cerrados para los servidores y otros controles físicos de última generación de los cuales la mayoría de las empresas no dispone.

Obtenga más información

Consulte "Empowering developers through cloud services" y descubra los beneficios de Red Hat® Cloud Services para el desarrollo de las aplicaciones en la nube.

Acerca de Red Hat

Con Red Hat, los clientes pueden llevar la estandarización a todos los entornos, desarrollar aplicaciones directamente en la nube e integrar, automatizar, proteger y gestionar los entornos complejos a través de los servicios galardonados de soporte, capacitación y consultoría.

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

ARGENTINA
+54 11 4329 7300

CHILE
+562 2597 7000

COLOMBIA
+571 508 8631
+52 55 8851 6400

MÉXICO
+52 55 8851 6400

ESPAÑA
+34 914 148 800

es.redhat.com
#F31540_0522