Cómo generar confianza en un cielo lleno de nubes

Los servicios en la nube son ya parte integrante habitual de las operaciones de TI, y se utilizan en más del 90 % de las empresas de todo el mundo. Muchos aplican una filosofía que da prioridad a la nube (conocida como "Cloud First") y solo deciden desplegar un servicio interno cuando no hay una variante en la nube adecuada disponible. Como resultado, las arquitecturas de TI están pasando rápidamente a un modelo de nube privada/pública híbrida; los encuestados prevén que el 80 % de su presupuesto para TI se destine a la nube en un plazo medio de 15 meses.

El **93 %** de las empresas **utilizan servicios en la nube** de alguna forma.

El **49 %** de los encuestados **redujeron la adopción de la nube** debido a la falta de expertos en ciberseguridad.

El **62 %** de las empresas manifestaron que **almacenan información personal de los clientes** en las nubes públicas.

Intel Security encuestó a más de 2000 profesionales de las tecnologías de la información en septiembre de 2016 para generar este informe anual del estado de la adopción de la nube, lo que representa un amplio espectro de sectores, países y tamaños de empresas. El impacto que la escasez continua de personal de seguridad cualificado ha tenido en la adopción de la nube ha sido un tema prioritario para el informe de este año. Otros objetivos eran conocer la adopción de distintos modelos de uso de la nube, identificar las preocupaciones principales que suscitan los servicios en la nube privados y públicos, e investigar el impacto del uso de aplicaciones que no cuentan con la aprobación del departamento de TI (lo que se conoce como "TI en la sombra").

Los participantes en la investigación son responsables de la toma de decisiones de pequeñas (500 - 1000 empleados), medianas (1000 - 5000 empleados) y grandes (más de 5000 empleados) empresas, ubicadas en Alemania, Australia, Arabia Saudí y Emiratos Árabes Unidos, Brasil, Canadá, Estados Unidos, Francia, Japón, México, Reino Unido y Singapur.

Conclusiones principales

- Los servicios en la nube se utilizan ampliamente de distintas formas; el 93 % de las empresas utilizan el software como servicio, la infraestructura como servicio o la plataforma como servicio.
- El número promedio de servicios en la nube que se emplean en una empresa descendió de 43 en 2015 a 29 en 2016, lo que indica una consolidación potencial de proveedores o soluciones en la nube. Las arquitecturas en la nube también cambiaron sustancialmente, pasando del uso de las eminentemente privadas en 2015 a una mayor adopción de la nube pública, lo que dio lugar a una infraestructura pública/privada híbrida en 2016.
- Casi la mitad (49 %) de los profesionales encuestados manifestaron haber reducido la adopción de la nube debido a la escasez de expertos en ciberseguridad. Los países más afectados son Japón, México y los países del Golfo Pérsico.
- La confianza y la percepción de los servicios en la nube pública siguen mejorando año tras año. La mayor parte de las empresas ven los servicios en la nube como igual o más seguros que las nubes privadas y consideran que ofrecen muchas más posibilidades de reducir los costos de propiedad y mejorar la visibilidad global de los datos. Ahora el número de los que confían en las nubes públicas supera al de los que desconfían en más del doble.

Resumen ejecutivo

El **52 %**

de los encuestados asociaron una **infección de malware a una aplicación SaaS**.

El **40 %**

de los servicios en la nube han sido **encargados sin intervención de TI**.

El **65%**

de los profesionales de TI creen que **la nube en la sombra interfiere** en su capacidad para garantizar la seguridad de la nube.

2 años

Plazo tras el cual esperan los encuestados tener un **centro de datos totalmente definido por software**.

- La mejora de la confianza y la percepción, así como un mayor conocimiento de los riesgos por parte de los directivos, animan a más organizaciones a almacenar los datos confidenciales en la nube pública. Los datos que más se almacenan en la nube pública son la información personal de los clientes, como afirman hacer el 62 % de los encuestados.
- Las aplicaciones en la nube siguen siendo un vector de ciberataques y más de la mitad de los encuestados (52 %) indican que pueden atribuir con certeza una infección de malware a una aplicación SaaS.
- El TI en la sombra cada vez preocupa más al departamento de TI. Debido a la menor adopción de TI o a la aceptación generalizada de las nubes, casi el 40 % de los servicios en la nube se encargan sin ninguna participación de TI. Como resultado, el 65 % de los profesionales de TI creen que este fenómeno interfiere en su capacidad para garantizar la protección y la seguridad de la nube.
- La virtualización de las arquitecturas de centros de datos privados avanza. De media, el 52 % de los servidores de centros de datos de una empresa están virtualizados y la mayoría esperan haber finalizado la conversión a un centro de datos totalmente definido por software en un plazo de 2 años.

Conclusiones y recomendaciones

Las empresas confían a los servicios en la nube una gran variedad de aplicaciones y datos, una buena parte de los cuales son confidenciales o esenciales para el negocio. Los datos van allí donde se necesitan, y donde son más eficaces y más eficientes, y es necesario contar con seguridad preparada para detectar amenazas rápidamente, proteger la empresa y corregir los intentos de poner en riesgo los datos. El ahorro de costos y recursos que ofrecen los servicios en la nube es real y la amplia variedad de ofertas disponibles permite elegir los más adecuados para su empresa. Los proveedores de seguridad ofrecen herramientas que abordan las preocupaciones de seguridad fundamentales, como la protección de los datos en tránsito, la administración del acceso de los usuarios y la configuración de directivas coherentes en distintos servicios.

El traslado de datos confidenciales a la nube pública puede atraer a los ciberdelincuentes. Los agresores buscarán los objetivos más fáciles, independientemente de dónde se encuentren. Las soluciones de seguridad integradas o unificadas son una defensa eficaz frente a estas amenazas, que ofrecen a las operaciones de seguridad visibilidad de todos los servicios de la empresa y permiten determinar los conjuntos de datos autorizados para atravesarla.

Las credenciales de los usuarios, especialmente las de los administradores, serán el medio más habitual para ejecutar los ataques. Las organizaciones deben utilizar las mejores prácticas de autenticación, como por ejemplo, no repetir las contraseñas, o utilizar autenticación multifactor e incluso biometría.

A pesar de la idea extendida de que las TI en la sombra supone un riesgo para las empresas, las tecnologías de seguridad, como la prevención de pérdida de datos (DLP), el cifrado y los agentes de seguridad de acceso a la nube (CASB) siguen estando infrautilizadas. La integración de estas herramientas con un sistema de seguridad existente incrementa la visibilidad, facilita el descubrimiento de servicios en la sombra y proporciona opciones para la protección automática de datos confidenciales, ya estén en reposo o en movimiento y en cualquier tipo de entorno.

Si bien es posible externalizar el trabajo a terceros, no se puede externalizar el riesgo. Las empresas necesitan evolucionar hacia un enfoque de gestión y mitigación de riesgos de la seguridad de la información. Plantéese adoptar una estrategia que priorice la nube para reducir costos y aumentar la flexibilidad, y aplique a las operaciones de seguridad una actitud proactiva, en lugar de una reactiva.

Encontrará el informe completo para descargarlo **aquí**.

intel Security

McAfee. Part of Intel Security.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com