

Cómo estar seguros en la ‘Nube’

Parte I: Apocalípticos y entusiastas – Ventajas del modelo – Nuevos riesgos potenciales.

El modelo de entrega sobre el que descansan las clouds públicas, y por tanto también las clouds híbridas público/privado, al llevar a la ‘nube’ total o parcialmente los recursos TI corporativos siguiendo un enfoque multicliente bajo el control de un tercero exige un replanteamiento integral de la seguridad en aspectos como gestión, protección, accesibilidad y privacidad de la información. Pero ello no significa necesariamente que los servicios cloud sólo introduzcan riesgos. Aunque para una buena parte de expertos la seguridad sigue siendo la gran barrera para la adopción de Cloud Computing, para otros la propia naturaleza del nuevo modelo también aporta ventajas en este terreno. Se podría decir que es ésta una de esas controversias típicas que suelen envolver prácticamente a todas las tendencias tecnológicas hasta que se consolidan, consiguen dar respuesta a sus retos intrínsecos y logran finalmente una adopción masiva.

“Será un reto constante y un área de continuas innovaciones no sólo técnicas sino también en comunicaciones. Hay quienes piensan que Cloud Computing es muy seguro, otros que no lo es y no faltan los que no dan demasiada importancia a estas cosas. ¿Podemos ofrecer a los usuarios las herramientas que les hagan sentir que tienen el control, que les permita sentirse responsables? Pienso que los usuarios reconocerán la seguridad cloud cuando la vean. El problema justo ahora es que no saben realmente qué está pasando (en la ‘nube’)... y crear las herramientas y tecnologías que permitan gestionar fácilmente las interacciones es fundamental”. Estas palabras de Steve Ballmer, CEO de Microsoft, pronunciadas el pasado mes de marzo durante una conferencia en la Universidad de Washington, reflejan fielmente la verdadera situación en la que se encuentran los usuarios frente a las propuestas de Cloud Computing: si sus ventajas son incuestionables, también sus debilidades potenciales, y por encima de cualquier otra, los nuevos retos de seguridad que introduce.

CRECE LA CONFIANZA

A medida que los servicios cloud evolucionan y maduran, crece también el grado de confianza en la ‘nube’. El informe ‘Treta Bryson Reporta’ realizado recientemente por Información Security Forum (ISF) entre 300 de las principales compañías y organizaciones del sector público de todo el mundo concluye que, pese a que Cloud Computing implica un cambio en el panorama de riesgos de seguridad a que deben enfrentarse, el 90% de los sondeados afirman sentirse en condiciones de poder afrontarlo con éxito. Un optimismo similar respira un informe de Penteo publicado el pasado junio, donde se revela que las empresas españolas que utilizan en la actualidad algún servicio cloud reconocen un elevado nivel de satisfacción respecto a seguridad y privacidad. La nota más alta de satisfacción recae en la posibilidad de compatibilizar modelos cloud con el cumplimiento de la Ley de Protección de Datos (LOPD).

Otras prospecciones sin embargo no muestran un panorama tan alentador. Según los resultados de un reciente sondeo realizado por TPI, consultora

especializada en outsourcing, de los factores que preocupan a las empresas e impiden que

“Las empresas españolas que utilizan actualmente algún servicio Cloud reconocen un elevado nivel de satisfacción respecto a seguridad y privacidad”

(Fuente: Penteo –Junio 2010-)

decidan migrar recursos más importantes al nuevo modelo, el 79% de los sondeados señaló, de entre varias posibilidades, la ‘inadecuada’ o ‘no del todo clara’ seguridad de los datos, mientras que un 50% apuntó los requisitos de conformidad normativa y un 50% la recuperación de desastres y la continuidad de negocio. Los defensores de Cloud Computing, en cualquier caso, tienen claro que en lo que se refiere a seguridad el nuevo modelo también ofrece ventajas. La tecnología de virtualización que forma la base de los servicios cloud es una de ellas. Un servicio cloud basado en máquinas virtuales compartidas por varios clientes aporta altos niveles

de disponibilidad no comparables con los que ofrecen los servidores dedicados. Al disponer de un pool de máquinas virtuales, si un nodo físico se viene abajo, es posible mantener activa la operación de forma automatizada en otro lado de la 'nube'.

”Asimismo, almacenar datos en múltiples servidores distribuidos en diversas ubicaciones dificulta a los cibercriminales conseguir sus objetivos”

Asimismo, almacenar datos en múltiples servidores distribuidos en diversa ubicaciones dificulta a los cibercriminales conseguir sus objetivos, además de proporcionar redundancia para protegerse contra desastres.

También permite responder a los ataques más rápidamente al reducir el tiempo de instalación de

parches sobre miles de desktops individuales o cientos de servidores internos.

No es desdeñable tampoco la ventaja que supone disponer de los departamentos y equipos de los proveedores dedicados 24x7 a proteger la información sensible de los clientes y encontrar continuas mejoras para su seguridad, monitorización, prevención de intrusiones... Así, organizaciones pequeñas y medianas pueden disfrutar de las mismas ventajas que las grandes compañías sólo que con un entorno multicliente.

Hasta la GAO (Government Accountability Office) de Estados Unidos, que estudia los riesgos potenciales de Cloud Computing para las agencias gubernamentales del país, concede que la virtualización y automatización en que se basa el modelo aporta interesantes ventajas. Dos de ellas son la aceleración del despliegue de configuraciones seguras para imágenes de máquinas virtuales y la capacidad de aplicar controles de seguridad bajo demanda.

PUNTOS FUERTES.

ENISA (European Network and Information Security Agency) publicó en 2009 el documento 'Cloud computing. Benefits, risks and recomendations for information security', donde recoge en siete categorías las principales ventajas que los servicios cloud aportan en seguridad:

Beneficios de escala. Implementar medidas de seguridad es más económico cuando se hace a gran escala. Tales medidas abarcan desde filtrado a gestión de parches y protección de instancias de máquina virtual. Asimismo se puede disfrutar de las ventajas que supone disponer de múltiples ubicaciones, redes de extremo, tiempos de respuesta a incidentes, etc.

Interfaces estandarizados. Los grandes proveedores de cloud pueden ofrecer una interfaz abierta y estandarizada que mejora la disponibilidad de los servicios de seguridad.

Escalado rápido e inteligente de recursos. El proveedor puede dinámicamente asignar recursos para tareas como filtrado, formación del tráfico, autenticación, encriptación, protección contra ataques DoSS.

Auditoría. Cloud Computing puede proporcionar 'imágenes' de pago por uso de máquinas virtuales sin necesidad de desactivar la infraestructura, lo supone un menor tiempo de inactividad para realizar análisis forenses, entre otras cosas.

Actualizaciones y respuesta a fallos más eficientes y rápidas. Los fallos de las imágenes virtuales y de los módulos de software usados por los clientes pueden ser reparados y actualizados con los últimos parches y soluciones de seguridad siguiendo procesos optimizados.

Beneficios de la concentración de recursos. Aunque la concentración de recursos implica riesgos, también permite disponer de un control de accesos y perimetrización físicos más baratos, así como procesos relacionados con seguridad más sencillos y económicos.

Seguridad como factor diferenciador. Como la seguridad es una prioridad para muchos clientes de cloud, los proveedores se esfuerzan en basar su reputación en disponer de altos niveles de confidencialidad, integridad y resiliencia.

VISIÓN GLOBAL DE LOS NUEVOS RETOS.

Pese a todo, estas ventajas de Cloud Computing tienen su contrapartida en otros tantos retos de seguridad de los que las compañías se tendrán que proteger adoptando un enfoque estratégico global que comprenda todos los frentes en riesgo. Fusionando los principales riesgos específicos del modelo identificados por ENISA con las conclusiones del documento 'Top Threats to Cloud Computing' versión 1.0 publicado el pasado diciembre por Cloud Security Alliance y las principales contribuciones de expertos y consultoras sobre algunos aspectos específicos, la siguiente clasificación ofrece una visión global del problema.

Pérdida de control. En los servicios cloud el cliente necesariamente cede el control al proveedor sobre determinados aspectos que pueden afectar a la seguridad y que los SLA deberían contemplar en detalle. Un efecto indeseable de esta pérdida o cesión del control se produce cuando, por la falta de formatos, procesos e interfaces estándar que garanticen la portabilidad del servicio, la aplicación o los datos del cliente entre distintos proveedores. Es decir, se corre el riesgo de quedar bloqueado en manos del proveedor seleccionado.

Recursos compartidos. La naturaleza compartida de Cloud Computing está expuesta a potenciales fallos en los mecanismos de separación de los diferentes recursos de almacenamiento, memoria o routing entre los distintos clientes, como los conocidos como ataques guest-hopping, poco numerosos todavía pero siempre posibles. Cloud Computing Security Alliance recuerda además que en los servicios IaaS los hipervisores de virtualización pueden mostrar niveles inapropiados de control. Una estrategia de defensa profunda en este apartado debería incluir técnicas que impidan que las distintas actividades de los clientes interfieran entre sí. Para la Alianza, se deberían garantizar además potentes procesos de autenticación y control de accesos, y potentes SLA sobre parches, auditorías de configuración y escaneo de vulnerabilidades, entre otras medidas.

Protección de datos y conformidad normativa. Los datos se pueden ver comprometidos de muchas formas, ya sea por eliminación o alteración, o por pérdidas y filtraciones. Riesgos que en la 'nube' se ven incrementados debido al elevado número de interacciones y a las propias características de los servicios cloud, más expuestos a accesos no autorizados. Para evitarlos se han de implementar potentes mecanismos de control de autenticación, autorización y auditoría de accesos, la encriptación de los datos en tránsito y estrategias efectivas de retención y backup. Un problema relacionado es la conformidad normativa, que, según ENISA, puede verse en riesgo si el proveedor no proporciona evidencias de su propio cumplimiento de los requisitos más relevantes y si no permite al cliente realizar sus propias auditorías.

API e interfaces inseguros. La seguridad y disponibilidad de los servicios cloud dependen de la seguridad de las API e interfaces que los clientes utilizan para gestionar e interactuar con ellos. Por ello estas interfaces deben ser diseñadas para evitar intentos accidentales o maliciosos de burlar las políticas. Cloud Security Alliance resalta la importancia de la interfaces de gestión del cliente, que al ser accesibles a través de Internet y dar acceso a grandes conjuntos de recursos, suponen un riesgo incremental cuando se combina con el acceso remoto y los navegadores web.

Ataques internos y externos. Aprovechando el relativo anonimato de los modelos de uso y registro de los servicios cloud, spammer, autores de código malicioso y otros criminales pueden llegar a conseguir una cierta impunidad. Cada vez tendrán más presencia acciones como el robo de claves y contraseñas, DDOS, hosting de datos maliciosos o botnets, entre otros muchos. ENISA recuerda en este sentido el peligro creciente de los ataques internos.

Con estos riesgos en mente, las compañías deben de crear una estrategia de seguridad cloud que se adapte a las peculiaridades de sus entornos y a las demandas de su negocio, y, de acuerdo a ella, buscar el proveedor que le ofrezca mayores garantías en el cumplimiento de estrictas medidas de protección.

“Si un proveedor de Cloud no proporciona información suficiente sobre sus planes y procesos de seguridad, no se debería confiar en él”

(Fuente: Nemertes Research)

Quizá una buena manera de empezar a migrar a la ‘nube’ sea probar inicialmente con aplicaciones y partes no críticas de la infraestructura corporativa

para ir aprendiendo del nuevo modelo sin exponerse a grandes riesgos. En cualquier caso, las empresas deben de acercarse a Cloud Computing exigiendo la máxima transparencia. Es habitual que los proveedores de servicios en la ‘nube’ se muevan con cierto secretismo sobre sus centros de datos y sus operaciones, asegurando que así se garantiza mejor la seguridad. Pero, como advierte Nemertes Research, si un proveedor de servicios no proporciona la información suficiente sobre sus planes y procesos de seguridad, no se debería confiar en él.

Esta última apreciación conduce a la importancia que tiene la selección del proveedor de Cloud Computing adecuado, tema que junto a los estándares, certificaciones y avances en la seguridad del modelo, serán tratados en la segunda parte del presente documento.