ISEC Labs #8

¿Nubes o nubarrones? Seguridad en Cloud Computing

Javier Moreno
jmoreno<arroba>isecauditors.com

1. Introducción

Cloud Computing ha llegado, o siendo más rigurosos ha vuelto (¿quién no recuerda los tiempos de terminales "tontos" conectados a ordenadores centrales?) para instaurarse definitivamente en el mundo de las tecnologías de la información. El modelo Cloud Computing permite ofrecer cualquier servicio informático a través de Internet ofreciendo al cliente una capa de abstracción sobre los recursos que se están utilizando. Cloud Computing ofrece a sus usuarios un interesante ahorro de costes frente a soluciones tradicionales ya que se beneficia de las economías de escala procedentes del uso compartido de recursos. Sin embargo, desde el punto de vista de la seguridad de la información surgen una serie de interrogantes acerca de las distintas amenazas que acechan al Cloud Computing.

2. Conceptos

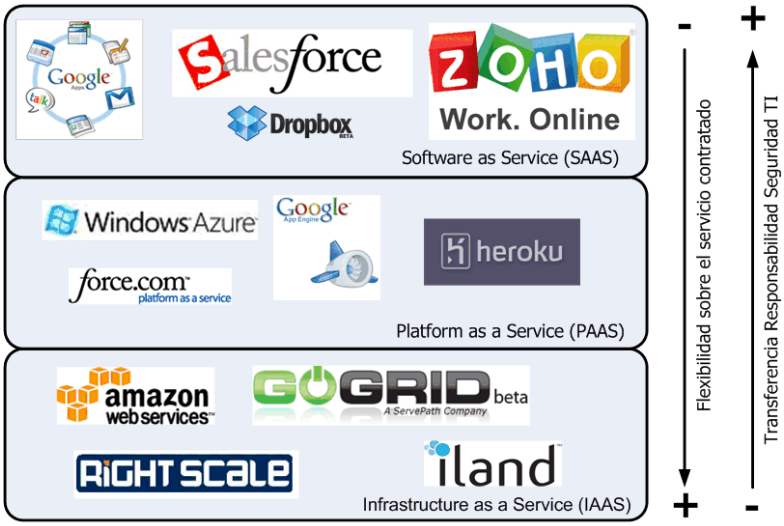
Para poder entender las amenazas y fortalezas del Cloud Computing en lo que a Seguridad de la Información se refiere, es necesario conocer su principales características: su alto nivel de abstracción, la satisfacción de necesidades bajo demanda, la reducción de costes debido al uso de economías de escala, el pago por uso, la escalabilidad de la soluciones ofrecidas y la provisión de los servicios de forma instantánea.

Dentro del paraguas del Cloud Computing, se encuentran 3 modelos de servicio claramente diferenciados [1]. La modalidad de servicio Cloud más conocida es SaaS (Software as Service). En este modelo el cliente usa aplicaciones que están ejecutándose en la infraestructura Cloud del cliente. El principal inconveniente de esta modalidad es que la flexibilidad del cliente se limita a la configuración de unas pocas características en la aplicación. Como ventaja, cabe destacar la transferencia al proveedor de casi todos los aspectos relacionados con la seguridad TI.

El segundo modelo de servicio de Cloud Computing es PaaS (Platform as a Service). En este caso el cliente despliega sus aplicaciones sobre la infraestructura del proveedor. Las aplicaciones del cliente tienen que estar desarrolladas en tecnologías y lenguajes soportados por el proveedor Cloud. En este modelo, el cliente tiene el control de su aplicación y la responsabilidad sobre la seguridad de la misma a nivel 7; sin embargo no puede realizar cambios en la configuración de red, sistemas operativos o almacenamiento.

El tercer y último modelo de servicio del Cloud Computing es el denominado IaaS (Infrastructure as a Service). En este modelo al cliente se le presenta la posibilidad de adquirir (alquilar) procesamiento, almacenamiento, recursos de red y cualquier otro tipología de infraestructura tecnológica. El cliente despliega en la infraestructura contratada el software que estime necesario: desde sistemas operativos a simples aplicaciones. El cliente tiene el control casi total sobre la infraestructura contratada y por tanto apenas hay transferencia de responsabilidad de la seguridad al proveedor.

La Figura 1 muestra algunos ejemplos de proveedores de servicios clasificados según su modelo de servicio. En el gráfico también se observa como la flexibilidad de la que dispone el cliente en los servicios contratados es inversamente proporcional a la responsabilidad sobre la seguridad TI transferida al proveedor del servicio Cloud [2].



3. Amenazas a la Seguridad de la Información del Cloud Computing

Según un estudio realizado por IDC en Agosto de 2008 [3], la seguridad es el reto más importante que los responsables de informática encuentran para adoptar soluciones y servicios Cloud Computing. Las principales amenazas de este modelo [4] se pueden agrupar en la siguiente clasificación:

1. Bloqueo en proveedores
2. Actualmente no existe una gran variedad de proveedores de servicios Cloud. Un cliente puede tener muchas dificultades al intentar cambiar de proveedor de servicios Cloud Computing.
3. Fallo de aislamiento
4. El uso compartido de recursos es una de las características más importantes del Cloud Computing. Si el aislamiento de los clientes no es lo suficientemente bueno, podrían ocurrir "invasiones" entre clientes.
5. Riesgos de cumplimiento
6. Al externalizar ciertos servicios y procesos básicos, el cumplimiento legislativo (LOPD) y normativo (PCI DSS, ISO 27001,â€¦) se complica.
7. Publicación de los interfaces de gestión
8. Los interfaces de gestión de los servicios Cloud están normalmente publicados en Internet. Este hecho incrementa el riesgo de pérdida o robo de información.
9. Borrado de datos inseguro o incompleto
10. La reutilización de recursos hardware es muy habitual en el Cloud Computing. A un nuevo cliente se le puede asignar, por ejemplo, una sección de almacenamiento en la que hasta hace poco se encontraban datos de otro cliente. Si el borrado de información no se ha realizado correctamente, la confidencialidad de los mismos corre peligro.
11. Administradores muy privilegiados
12. El Cloud Computing necesita, para su administración, perfiles de usuario muy altos. Un administrador de sistema tendrá grandes privilegios sobre distintos recursos de distintos clientes. Un usuario malévolo que consiga capturar una sesión de administrador tendrá a su disposición la información de muchos clientes.

4. Fortalezas en la Seguridad del Cloud Computing

Aun viendo que las amenazas que se ciernen sobre el Cloud Computing son muchas y muy graves, es justo destacar que este modelo de computación añade una serie de ventajas a la gestión de la seguridad de la información [5]:

1. Pre-hardenización
2. Debido a que los servicios Cloud se replican con mucha facilidad, un nuevo cliente encontrará un entorno correctamente asegurado, hardenizado y testeado desde el inicio.
3. Centralización de los datos
4. La congregación de recursos en una misma localización conlleva una reducción de costes sobre la seguridad perimetral y el control de acceso físico.
5. Economía de escalas enfocadas a elementos de seguridad.
6. Elementos de gestión de seguridad de la información como la gestión de parches, la hardenización de sistemas o la implantación de filtros requiere muchísima menos inversión en Cloud Computing debido a que estos recursos se comparten entre clientes.
7. Rápida respuesta ante incidentes
8. Ante un incidente en el que se vea afectada la disponibilidad de los sistemas del cliente, un proveedor de servicios o incluso el cliente, puede reubicar sus sistemas y/o servicios en otra parte de la infraestructura Cloud que no se haya visto comprometida.
9. Seguridad como valor añadido al servicio
10. Los proveedores de seguridad tienen en el Cloud Computing una oportunidad de oro para generar valor en sus servicios. "La nube será lo mejor que le ha podido pasar a la industria de la seguridad", afirmó Andrew Jaquith, analista senior de Forrester, en la VI jornada internacional organizada por el ISMS Forum Spain [6].
11. Gestión y almacenamiento de logs.

12. El modelo de pago por uso que presenta Cloud Computing, permite superar los problemas de almacenamiento y procesamiento asociados históricamente a la gestión de logs.
13. Facilidad para la realización de auditorías
14. La ejecución de herramientas de auditoría automáticas, así como, la búsqueda manual de vulnerabilidades se simplifica debido a la replicación de entornos existente en el modelo Cloud Computing.

5. Conclusiones

El fenómeno Cloud Computing es imparable. Los responsables de seguridad (CISO) de las compañías ven con recelo la seguridad de este modelo, sin embargo, el ahorro de costes que conlleva hacen que los CEOs y CFOs miren con muy buenos ojos su implantación. Será tarea de los CISOs resolver las distintas problemáticas relacionadas con la seguridad TI en el Cloud Computing, permitiendo así un gran ahorro de costes a sus organizaciones con el reconocimiento interno que esto implica. El Cloud Computing es una oportunidad única para alinear las tecnologías de información con uno de los objetivos principales de cualquier empresa, el ahorro de costes. El único impedimento para conseguir esta combinación es la seguridad, debemos superarlo.

6. Referencias

- [1] Wikipedia - Cloud Computing.
- [2] Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. Cloud Security Alliance.
- [3] IDC Enterprise Panel, August 2008.
- [4] Cloud Computing - Benefits and recommendations for information Security - November 2009. ENISA.
- [5] CloudSecurity.org.
- [6] Conclusiones VI Jornada Internacional ISMS Forum Spain, https://www.ismsforum.es/noticias/noticia.php?noticia=239.