Peligro Y Perdida Del Control En Could Computing ¿Existe Seguridad?

Liz Andrea Ramos Huarachi
Universidad Mayor De San Andres
Facultad de Ciencias Puras y Naturales
Carrera De Informática
Simulación de Sistemas
Aandrea_lian@hotmail.com

RESUMEN

Actualmente la computación en la nube (cloud computing) está muy presente en todas las empresas y representa un gran cambio, debido a que los clientes están emocionados con despojarse de la infraestructura que almacena toda su información y poder usar las aplicaciones en servicios alojados de forma externa, es decir en la propia web, todo esto esta alcanzando una gran popularidad, y por lo mismo deberían surgir preocupaciones sobre los problemas de seguridad en este nuevo modelo.

Esta documentación presentará información sobre la seguridad en el could computing. La eficacia y eficiencia de los mecanismos tradicionales de protección están siendo reconsiderados por la gran cantidad de datos que se encuentran flotando en la nube y los principios de seguridad similares que se aplican en compartidos de varios usuarios de mainframe modelos de seguridad se aplican con seguridad en la nube.

Palabras clave

Seguridad: disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas orientados a proveer condiciones seguras para el procedimiento de datos en todo tipo de sistemas.
Amenaza:

1. INTRODUCCIÓN

Cloud Computing (Computación en la nube) no es un concepto muy novedoso, pero si las empresas quieren aumentar su capacidades competitivas deben pensar seriamente en la "NUBE" y buscar proveedores de servicios Cloud Computing, que logra fomentar la productividad, centralizando los recursos y el conocimiento de la empresa. Pero siempre se tiene que tener cuidado con la posible dependencia que se puede generar hacia los proveedores de servicios. La computación en nube significa que tenemos que confiar en las grandes empresas que presten los servicios para mantenernos a salvo y si algo les falla también nos afectara en gran medida
.
La cantidad de empresas que ofrecen servicios de aplicaciones en la Web está en aumento, como las redes sociales, prestando servicios e-mail, dirección, almacenamiento, herramientas de colaboración y aplicaciones de negocio los más grandes y más conocidos proveedores de Cloud Computing incluyen a Amazon con EC2, Microsoft con Azure y Google con Google Apps (p.ej. Gmail, Google Docs, Google Calendar)

2. COULD COMPUTING: pérdida del control

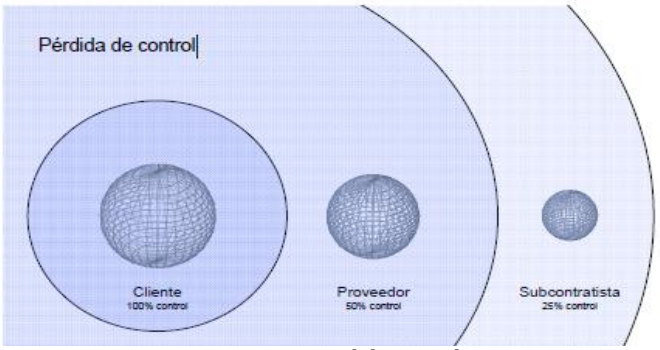

Figura 1. Nivel de control

Al dejar que nuestros datos y relaciones no estén en nuestros equipos, no dependan del sistema operativo de nuestros equipos, sino en la red (the cloud, en las nubes), estamos arriesgando mucho, por tal razón los proveedores deben seleccionar cuidadosamente los controles de seguridad adecuados.

Pero: ¿Qué significa? Que nuestros datos, aplicaciones y los servicios que utilizamos no estén en nuestros equipos ni dependan del sistema operativo de nuestros equipos, si no en la red, de la nube. ¿En qué manos nos gustaría que estuviera nuestra información?

"Una de las razones por las que no debes usar aplicaciones web para tus tareas de TI, es que pierdes el control. Tú debes estar en condiciones de realizar tus propias tareas en tu propio PC, en un programa amante de la libertad. Si usas un programa propiedad de un proveedor, o el servidor Web de otra persona, entonces quedas indefenso…el cloud computing es una trampa"[1]

2.1. Posibles riesgos o amenazas[2]

Algunos riesgos o amenazas de esta situación son:

- Interfaces y APIs inseguras
- Las vulnerabilidades tecnológicas compartidas
- Pérdida de los datos o fuga
- Secuestro de cuenta o servicio
- Transferencia de datos

Para trabajar con servicios de cloud computing necesitamos de una interfaz de software o APIs, y justamente la seguridad dependerá de cuan segura es la interfaz, por ejemplo con la autentificación, si otra persona logra acceder a su cuenta, este podría espiar sus actividades e incluso borrar información, por tal razón es importante replicar los

datos protegiéndolos de posibles fallos. Al momento de la autentificación se pueden usar dos estándares:

"SLAM: administrar usuarios previamente autentificados para el uso de todas la aplicaciones, proporcionando un entorno para el intercambio de información; XACML: controlar los accesos de los recursos"[3]

Al seleccionar un proveedor más que ver la aplicación que nos ofrece, se deber examinar la infraestructura, y que puede afectar directamente a la calidad y tecnología de la empresa-cliente, y al realizar el contrato la empresa debe definir en forma muy clara que todos los derechos sobre los datos o información solo le pertenecen a la empresa, comprobando las reglas bajo las que van a encontrarse los datos y su movimiento fuera de la compañía, ya que el proveedor de servicios puede tener acceso a los datos que están en la nube en cualquier punto en el tiempo

2.3. Seguridad

Dado que al usar cloud computing estamos poniendo en el especio todos nuestro datos e información y sabiendo que algunas veces hasta el más confiable respaldo llega a fallar, y cuando lo hace, los usuarios pueden llegar a perder todo, se necesita de mucha seguridad y sobre todo que la aplicación usada sea lo más segura posible.
"Los principios para la protección de la nube son la seguridad de la identidad, de la información y de la infraestructura"[4]

Se debe mantener lo más segura la identidad del usuario, sobre todo en el manejando de datos delicados, siendo persistentes en toda la infraestructura. Además de encritar dichos datos, utilizando software de buena calidad para ello y siempre hacer respaldos de los datos almacenados en la nube.

2.5. ¿Existe algún peligro?

"el cloud computing es la verdadera batalla importante en este momento en la escena tecnológica: las compañías que dominen "la nube" serán los verdaderos actores del futuro, con esquemas de concentración muy importantes debido a la misma naturaleza de la actividad"[5]

Varias empresas de internet están creando aplicaciones cloud permitiendo acceder a la información o datos de la empresa desde cualquier parte y dispositivo, además que la capacidad de almacenamiento es mucho mayor a la de un dispositivo físico, pero siempre estará el peligro de perder el control de dichos datos, el proveedor que gestiona el servicio se quiera o no tiene cierto grado de control sobre la información y si existe o se produce algún fallo respecto a la información por lo general no se hace cargo.

3. CONCLUSIONES

El poder tener a tu computadora personal en la nube y poder llevarla a donde quiera que vayas, mantener nuestras aplicaciones abiertas las 24 horas del día y los 7 días de la semana accediendo a ellos desde cualquier computadora y todo prácticamente gratis, es algo revolucionario sobre todo para los departamentos de IT de las empresas, si bien antes se hablaba del miedo de que tus datos sean robados y que tus aplicaciones sean inestables, actualmente la eficacia y efectividad de sus servicios y ahorro económico del CLOUD COMPUTIN son las principales causas que varias empresas estén optando por su uso.

Pero sin perder de vista que una de las dificultades o problemas de Cloud Computing es la posible pérdida de control de los datos y dependencia de los proveedores, sino se realiza un adecuado acuerdo con dichos proveedores.

4. REFERENCIAS

[1]http://ictreview.blogspot.com/2008/10/cloud-computing-according-to-richard.html

[2]https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[3]http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

[4]http://www.rsa.com/solutions/business/wp/11021_CLOUD_WP_0209_SP.pdf

[5]http://lolap.wordpress.com/tag/cloud-computing/