Seguridad En La Nube

Erick Arminio Alvarez Velasquez
Universidad Mayor de San Andres
Facultad de Ciencias Puras y Naturales
Informática
Simulación de Sistemas
dive777@gmail.com

RESUMEN

La computación en la nube hoy en día es la tecnología más atrayente debido a la eficiencia, costo y flexibilidad. Sin embargo a pesar del interés que se genera hay todavía muchas inquietudes significativas para tomarlo como modelo para implementar en su totalidad.

Una de las inquietudes es que la información está dentro de la nube y debido a esto el propietario llega a perder el control de la misma, los usuarios deben tomar en cuenta las distintas implementaciones de seguridad que utilizan los distintos proveedores de nube, debido a que no existe una manera fácil de mudarse de un proveedor a otro, además que cada uno de los distintos proveedores provee una implementación distinta de la seguridad es recomendable ver cuál de todas estas, satisfacera todos los requerimientos de su empresa.

En este artículo se dará una visión general a lo que es la seguridad de la información y una explicación breve a las distintas ventajas, desventajas y vulnerabilidades que existen en la computación en la nube.

Palabras Clave

Computación en la nube, proveedor de nube, seguridad, ventajas, desventajas, vulnerabilidades.

1. INTRODUCCION

En este artículo se hablara de la seguridad en términos de seguridad de la información, esta seguridad es las precauciones que se tienen en las empresas que proveen computación en la nube, de manera que la información cumpla con tres principios: la confidencialidad, la disponibilidad y la integridad.

La computación en la nube empezó a construirse a principios de los 90. La idea principal de la computación en la nube es el separar al sistema de la infraestructura y los mecanismos de los que está compuesto, separándolo de las aplicaciones y servicios que ofrece.[1]

Ahora la pregunta que nos planteamos es: ¿Que es la computación en la nube?

Bueno en una corta explicación a grandes rasgos, la computación en la nube es software y hardware que esta hospedado en un ambiente centralizado que puede ser alquilado, de esta manera el usuario se convierte en un cliente ligero y acceder a los recursos independientemente del dispositivo que use.

Específicamente, la computación en la nube es un modelo de computación que tiene recursos virtualizados que se proveen como servicios o recursos sobre el internet. El concepto incorpora infraestructura como servicios, plataforma como servicio y software como servicio, así como las recientes tecnologías que tienen tema principal la confiabilidad sobre internet para satisfacer las necesidades de los usuarios. La computación en la nube provee comúnmente aplicaciones de negocios en línea, que son accesibles desde un navegador web (ver Figura 1).

Las nubes están diseñadas de manera que pueden escalar de manera sencilla, estar siempre disponibles y reducir el costo de operación. Esto se alcanza con la alta demanda de aplicaciones para múltiples usuarios, información y recursos de hardware (como por ejemplo la infraestructura de una red, recursos de almacenamiento y otros).

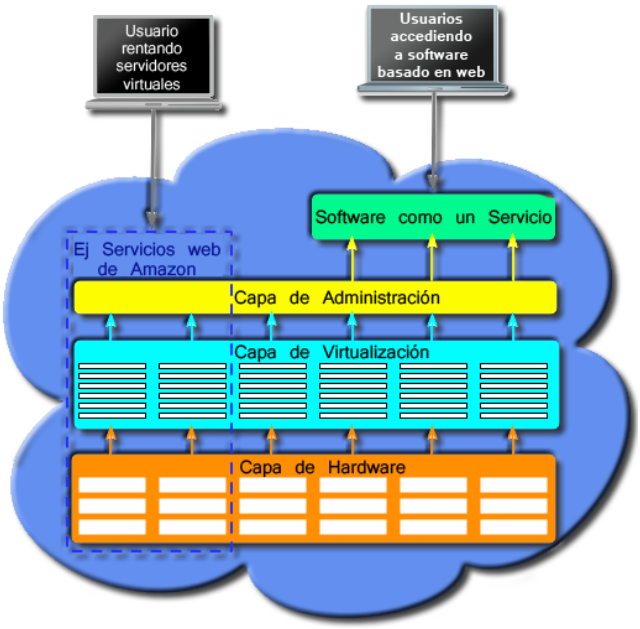

Figure 1. Implementación de la computación en la nube

2. SEGURIDAD

La seguridad de la información gano un gran terreno en la informática, ahora se pueden escoger distintas áreas de especialización, como por ejemplo en la auditoria de sistemas, planificación de negocios, informática forense y administración de sistemas.

Como principios básicos de la seguridad de la información se tiene a: La confidencialidad, la integridad y la disponibilidad.

La confidencialidad este principio asegura que la información no se divulgara o publicara a ninguna persona que no cuente con autorización, solo deberán tener acceso a la misma personas con autorización.

La integridad no permite cambios a la información por personas ajenas a la misma.

La Disponibilidad es la posibilidad de un usuario de ingresar a la información en cualquier momento que desee, sin importar el lugar donde se encuentre.

La manera en la que la seguridad esta implementada en la computación en la nube en la mayoría de los casos, es muy similar a la seguridad en los ambientes de Tecnologías de la información (TI) tradicionales. Pero debido a la naturaleza distribuida de los bienes, el riesgo de seguridad varía dependiendo en la clase de bien a usar, quien y como maneja esos bienes, cuales son los mecanismos de control a usar y cuando se encuentran localizados y finalmente quien consume los bienes.
Como mencionamos anteriormente que está diseñada para múltiples usuarios, se debe tener un set de políticas que deben ser implementadas para el aislamiento de recursos, facturación, segmentación y más, para alcanzar una forma concisa y segura.

Para poder verificar si la seguridad que el proveedor de la nube (PN) ofrece es la adecuada, debemos tener a consideración la madures, efectividad y la completitud del ajuste de riesgo de la seguridad que controla e implementa nuestro PN. La seguridad puede ser implementada en uno o más niveles. Estos niveles que cubren solo la infraestructura de la nube son: seguridad física, seguridad de red, seguridad de sistemas y seguridad de aplicaciones. Adicionalmente seguridad puede tener lugar en un nivel más alto, en las personas, obligaciones y procesos.

Es necesario en este punto que se entienda la diferencia de las responsabilidades de seguridad que tiene el PN y el usuario final. Algunas veces hasta entre los diferentes PNs las responsabilidades de seguridad varían.

A continuación se verán los distintos tipos de beneficios, riesgos y vulnerabilidades que se pueden llegar a tener al elegir un determinado proveedor de nube y ver la implementación de seguridad que el proveedor ofrece.

2.1. Beneficios de la seguridad

2.1.1. Seguridad y los beneficios de escalabilidad
Cuando se implementa la seguridad en un sistema grande el costo para su implementación es compartida por todos los recursos y como resultado de inversión termina siendo más efectiva y se ahorran costos.

2.1.2. La seguridad como diferenciador de mercado
Como la confidencialidad, integridad y la flexibilidad son una prioridad para muchos de los usuarios finales, la decisión en si ellos eligen a un PN en lugar de otro está basada en la reputación que tiene acerca de la seguridad la PN. Por lo tanto la competición entre las PNs hace que provean mejores niveles de servicios.

2.1.3. Recursos rápidamente escalables
La computación en la nube es considerada flexible debido a su habilidad de poder aumentar o reducir recursos. [3]

2.1.4. Auditoria y Reunir evidencia
Debido a que se usa la virtualización en muchas implementaciones en computación en la nube, es fácil recolectar toda la información necesaria para hacer auditorias para así poder proceder con el análisis forense de la información. [3]

2.1.5. Mayor tiempo, actualizaciones efectivas
Otro beneficio de la computación en la nube y la virtualización es que las máquinas virtuales pueden venir con las últimas actualizaciones. Además en caso de error o de desastres a causa de cambios en una máquina virtual, es posible deshacer el error y volver a un estado estable previo. [3]

2.1.6. Beneficios de la concentración de recursos
Al tener todos los recursos concentrados, los costos de mantenimiento rebajan y permite que un fácil acceso físico a los mismos. [3]

2.2. Riesgos de seguridad

2.2.1. Encerrado
Como se mencionó anteriormente todavía no hay estandarización en cómo mover la información y los recursos entre los diferentes PNs. Esto significa que en caso de que un usuario decida moverse de un PN a otro, no le será posible debido a las incompatibilidades que existen entre los PNs. Esto crea dependencia de los usuarios a un PN en particular. [2]

2.2.2. Fallo de aislamiento
Una de las desventajas de los recursos que son compartidos por múltiples usuarios ocurre cuando el mecanismo de aislamiento falla en separar los recursos entre los usuarios. Este problema se da por un ataque o debido a un mal diseño de mecanismo de aislamiento. En estos días los ataques de esta clase son muy raro comparados a los ataques tradicionales, pero no se puede asegurar en confiar solo en este hecho. La categoría de riesgo cubre la falla de mecanismos separando almacenamiento, memoria, ruteo e incluso entre diferentes arrendatarios. [2]

2.2.3. Riesgos de conformidad
Al usar una infraestructura de computación en la nube pública, no se podrá alcanzar la conformidad de los estándares de una industria. [2]

2.2.4. Administración de interfaces comprometida
Los diferentes PNs provén al usuario, administración de interfaces por sus recursos en infraestructuras públicas de nube. Haciendo que esas interfaces sean accesibles por internet permitiendo el acceso remoto a las aplicaciones o vulnerabilidades de los navegadores permitiendo el acceso a usuarios no autorizados. [2]

2.2.5. Protección de Información
Los PNs pueden manejar la información de maneras que no son conocidas por los usuarios, debido a que los usuarios pierden por completo el control de la información, pero existen algunos PNs que brindan información en como manejan la información, además de ofrecer certificación adicional en como procesan la información y de sus actividades de seguridad. [2]

2.2.6. Inseguro o información incompleta
Existen varios sistemas que a pedidos de eliminación de recursos no los eliminan completamente. También en el caso de la computación en la nube. Además de que surgen dificultades al eliminar un recurso debido a la existencia de copias de respaldo o razones de redundancia. Por estos casos de riesgo se añade protección a la información. [2]

2.2.7. Interno malicioso
Existe siempre la posibilidad de que alguien dentro de la PN cause daño. Por esta razón una política por roles específicos para cada usuario debe ser implementada. [2]

2.3. Vulnerabilidades

2.3.1. Vulnerabilidades AAA

Se debe tener cuidado especial en la autenticación, autorización y las cuentas de sistema que las PNs usaran. Un mal diseño de sistemas AAA puede resultar que usuarios no autorizados tengan acceso a los recursos, con malos resultados para la PN o los usuarios. [2]

2.3.2. Acceso remoto al manejo de interfaz

Teóricamente, esto permite vulnerabilidades en los terminales finales que comprometen la infraestructura de la nube. [2]

2.3.3. Vulnerabilidades de Hypervisor

En entornos de virtualización los hypervisores son una pequeña parte de middleware que se usa para poder controlar los recursos físicos asignados para cada máquina virtual. La explotación de las capas de los hypervisores puede resultar en explotar cada una de las máquinas virtuales existentes en el sistema físico. [2]

2.3.4. Vulnerabilidad en la encriptación de la comunicación

Mientras que la información se mueve a través del internet o entre diferentes lugares de los predios de la PN es posible que alguien pueda leer la información debido a mala autenticación. [2]

3.CONCLUSIONES

La computación en la nube es la tendencia que mayor impacto tiene hoy en día, debido a que facilita recursos y esto disminuye los costos para las empresas, sería prudente que se empiecen a desarrollar sistemas orientados a esta nueva tendencia, aunque muchos de los usuarios todavía temen que se perderá el control de información personal, importante o privada en la nube, estas personas deben tener en cuenta que para subsanar esto, las medidas de control de los proveedores de nube, implementaran y aplicaran nuevas técnicas de encriptación para la seguridad de la información. Estas medidas deberían alivianar en gran medida el miedo a la computación en la nube.

En este artículo se trató de explicar la seguridad en la nube y los distintos beneficios, desventajas y vulnerabilidades que existen, la computación en la nube es la tendencia de las tecnologías de la información más popular hoy en día, muchos piensan que es muy probable que la computación en la nube tendrá el mismo impacto que tuvo el software sobre el hardware. En opinión personal los modelos de computación en la nube están aquí para quedarse.

4.REFERENCIAS

1. Seguridad de la información <es.wikipedi.org/wiki/seguridad_de_la_informacion> [31-08-2012]
2. ENISA editors. (2009). Cloud Computing Benefits, risks and recommendations for information security. <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport> [31-08-2012]
3. Glenn Brunette and Rich Mogull (2009). Security Guidance for Critical Areas of Focus in Cloud Computing, Version 2.1 <http://cloudsecurityalliance.org/csaguide.p