Cloud Computing Security

Seguridad en Sistemas de Computación

FERMANI MAURO – CURCIO PABLO

Contenido

¿Qué es Cloud Computing?

Cloud Computing es un modelo de servicio por demanda, para la provisión de tecnología de información. Utiliza como soporte tecnologías de virtualización y de cómputo distribuido.

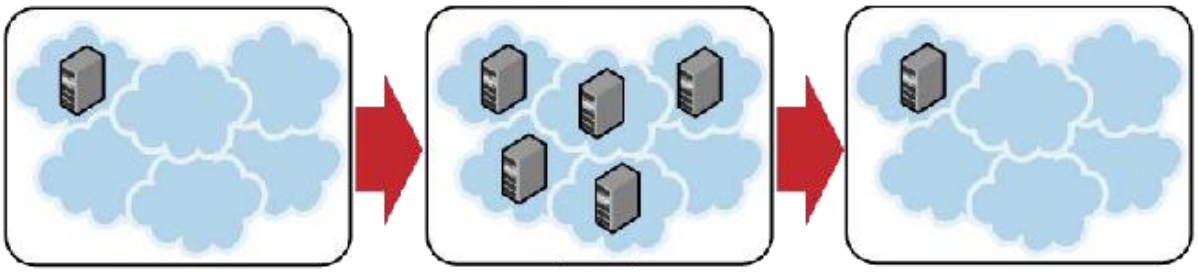
Las organizaciones pasan de generar y mantener sus propios sistemas de cómputo a adquirirlos como servicio

En su libro "The Big Switch" Nicholas Carr plantea una analogía entre el surgimiento del Cloud Computing y la red eléctrica. En un principio las organizaciones debían proveerse de su propia energía eléctrica. Luego, con la llegada de la red eléctrica, solo necesitaban conectarse a la misma para abastecerse, pudiendo concentrarse en su actividad principal y adquirir la energía como un servicio. Carr argumenta que el Cloud Computing es en realidad el principio de un cambio similar, donde las organizaciones pasan de generar y mantener sus propios sistemas de cómputo a adquirirlos como servicio a través de esta tecnología.

Atributos del Cloud Computing

El Cloud Computing se puede definir en base a los siguientes atributos:

- Alta escalabilidad: significa que puede adaptarse a una demanda creciente de recursos de cómputo que no está acotada, por ejemplo ancho de banda o almacenamiento. En el modelo tradicional, escalar el sistema puede implicar la necesidad de agregar hardware y soporte de tecnología de la información.
- Flexibilidad: permite a los usuarios incrementar o disminuir rápidamente los recursos de cómputo, pudiendo manejar picos de procesamiento, es decir, adaptar la cantidad de recursos disponibles a la demanda.



- Recursos compartidos: mediante virtualización, se abstraen los recursos físicos compartidos en recursos lógicos dedicados, a nivel de red, host y aplicación.
- Pay as you go: se paga en función de qué recursos se utilizaron y cuánto tiempo. Las aplicaciones tradicionales están basadas en un modelo con grandes costos de licencia que no están directamente relacionados con la utilización que se le da a la aplicación.
- Autoabastecimiento de recursos: lo usuarios pueden modificar su capacidad de procesamiento, almacenamiento, ancho de banda y adquirir software por sí mismos.

Tecnologías relevantes

El Cloud Computing en realidad no es una tecnología nueva, sino una combinación de varias preexistentes. Estas tecnologías que evolucionaron individualmente se han unido para soportar el concepto de Cloud Computing. Algunas de ellas son:

- Dispositivos de acceso a la nube: cada vez existen más dispositivos con capacidad de acceder a internet.
- Browsers y clientes finos: los usuarios pueden acceder a aplicaciones e información desde cualquier lugar capaz de cargar un browser. Se tiene una mayor disponibilidad de servicios que pueden ser accedidos a través de un cliente fino, en lugar de instalar una aplicación dedicada (cliente grueso) para acceder al mismo.
- Conexiones de alta velocidad: hoy en día se tiene gran disponibilidad de ancho de banda, que permite la interconexión de diferentes componentes y la creación de nuevos modelos de cómputo.
- Data centers: Los servicios basados en Cloud Computing necesitan gran capacidad de cómputo por lo que se hostean en data centers, que pueden abarcar varias ubicaciones interconectadas, proveyendo capacidad de distribución de cómputo y entrega de servicios.
- Dispositivos de almacenamiento: las nuevas tecnologías han reducido los costos y aumentado la flexibilidad de los dispositivos de almacenamiento. Las redes de área de almacenamiento (SANs) permiten la integración de varios dispositivos y asignar espacio por demanda.
- Virtualización: posibilita la creación de un pool escalable de recursos accesibles a través de métodos estandarizados, y la abstracción de los recursos físicos en lógicos ofreciendo una vista de recursos dedicados a los usuarios de la plataforma.
- Interfaces de programación de aplicaciones (APIs): Las APIs facilitan a los usuarios el autoabastecimiento y manejo de los recursos y servicios del cloud, enmascarando la complejidad.

Modelos de distribución de servicios de Cloud Computing

Los modelos de distribución de servicios de Cloud Computing, comúnmente referidos como SPI (Software – Plataform – Infrastructure) se clasifican en las siguientes categorías:

- Software as a Service (SaaS): Aplicaciones en la nube con tarifa mensual. Por ejemplo Google Docs, MobileMe, Zoho.
- Plataform as a Service (PaaS): Una plataforma que habilita a los desarrolladores a escribir aplicaciones que corran sobre la nube. Por ejemplo Microsoft Azure, Google App Engine, Force.com.
- Infrastructure as a Service (IaaS): Una infraestructura de cómputo compartida, redundante y escalable accesible a través de tecnologías de internet. Por ejemplo: Amazon EC2, Sun's cloud services, etc.

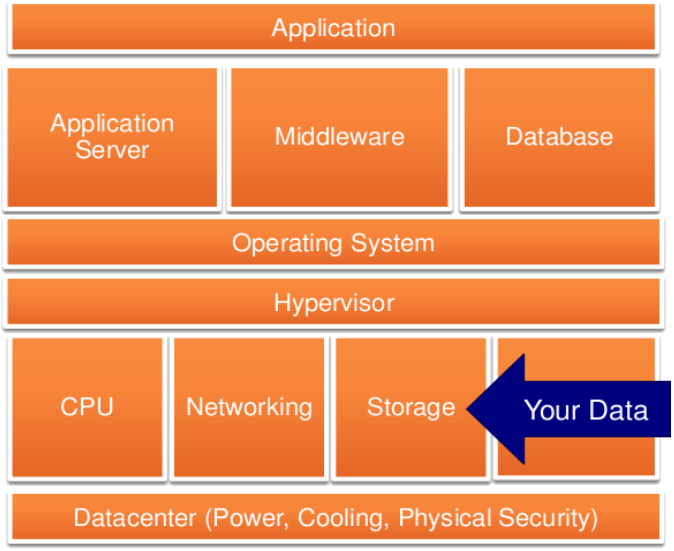
Software as a Service

La forma tradicional de adquirir software consistía en que los clientes compraran las licencias de las aplicaciones, servicios de soporte o mantenimiento y provean además el hardware donde las aplicaciones se ejecutarían.

En el modelo SaaS, el cliente paga por utilizar las aplicaciones del proveedor, que se ejecutan en la infraestructura del cloud. Generalmente el servicio comprado es completo en cuanto a hardware, software y soporte. Desde el punto de vista de la arquitectura, en el modelo SaaS la infraestructura de hardware es compartida por diferentes clientes, pero a nivel lógico es única para cada uno.

Entre las características ofrecidas por el SaaS se encuentran:

- El hosting y manejo de las aplicaciones puede ser realizado por terceros, reduciendo costos de licencias, servidores y otra infraestructura y personal necesarios para realizar el hosting en forma interna.
- El vendedor del software tiene mayor control sobre la copia y distribución del mismo, y se facilitan las actualizaciones.
- El acceso a la aplicación SaaS se realiza a través de un browser, aunque pueden existir casos en que los vendedores provean su propia interface para soportar características específicas de la aplicación.
- Generalmente es posible utilizar la infraestructura de acceso a internet existente, sin requerir hardware adicional, aunque puede ser necesario cambiar reglas en el firewall y realizar configuraciones.



En el modelo de servicio SaaS el cliente proporciona sus datos (azul) mientras que el proveedor es responsable del resto de los componentes (naranja).

Plataform as a Service

Es una variante del SaaS en la que el proveedor ofrece un entorno de desarrollo de aplicaciones como servicio, que es accedido por los desarrolladores a través de un browser. El entorno está hosteado en la infraestructura del cloud.

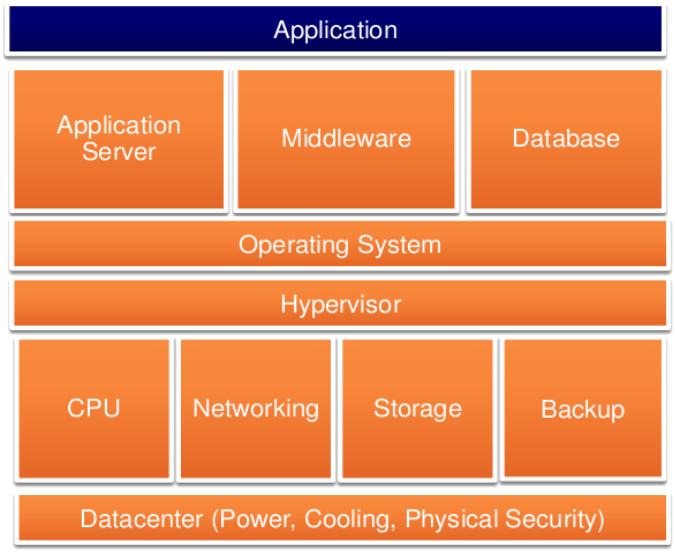
Las aplicaciones creadas por los usuarios pueden ser accedidas por sus clientes a través de la plataforma provista. El PaaS habilita a los desarrolladores a crear aplicaciones sin instalar herramientas en su computadora y a desplegarlas sin poseer conocimientos avanzados de administración de sistemas, evitando el costo y la complejidad de comprar servidores e instalarlos. El bajo costo inicial y las facilidades de desarrollo y despliegue permiten una rápida propagación de las aplicaciones.

Algunas de las características que debería ofrecer una alternativa PaaS son:

- Escalabilidad, confiabilidad, seguridad y multi-tenancy[1] sin requerir desarrollo adicional, configuración u otros costos por parte de los usuarios.
- Integración con bases de datos y servicios web externos.

[1] Capacidad de una aplicación de particionar el estado y los datos automáticamente para servir a un número arbitrario de usuarios

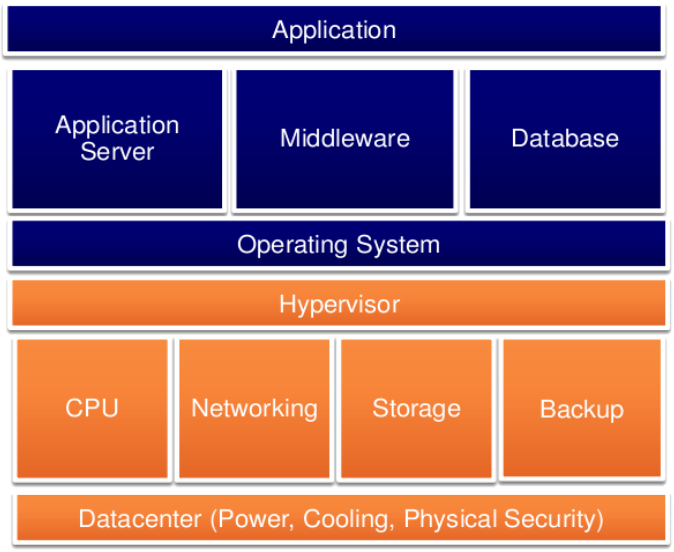
- Monitoreo de la aplicación y de la actividad de los usuarios para ayudar a los desarrolladores a hacer mejoras.
- Permitir la colaboración entre los desarrolladores durante el ciclo de vida del software y al mismo tiempo mantener la seguridad del código fuente y la propiedad intelectual asociada.
- Soporte de facturación de acuerdo al modelo pay-as-you-go.



En el modelo de servicio PaaS el proveedor se encarga de la infraestructura subyacente a la aplicación que desarrolla el cliente.

Infrastructure as a Service

En el modelo de servicio IaaS se provee la infraestructura necesaria para que el cliente desarrolle y ejecute software arbitrario, incluyendo procesamiento, almacenamiento, servicios de red y otros recursos de cómputos fundamentales. El cliente no administra ni controla la infraestructura del cloud subyacente al hypervisor, pero tiene control sobre los sistemas operativos, almacenamiento, las aplicaciones y algunas características de los componentes de red (por ejemplo, firewall de los sistemas operativos).



En el modelo de servicio IaaS el proveedor gestiona la infraestructura del Cloud necesaria para que el cliente desarrolle y ejecute software arbitrario.

Las principales características de un sistema típico de IaaS incluyen:

- Escalabilidad: tiene la capacidad de escalar la infraestructura, por ejemplo memoria y almacenamiento, basado en los requerimientos de uso.

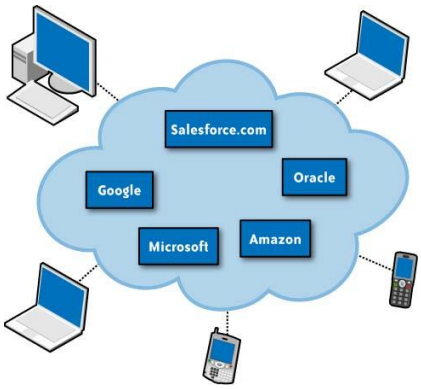
- Pay as you go: capacidad de adquirir la cantidad exacta de infraestructura requerida en un momento dado.
- Acceso a mejores soluciones de tecnología a una fracción de su costo.

Modelos de despliegue de Cloud Computing

Independientemente del modelo de servicio utilizado (SaaS, PaaS, IaaS) existen cuatro modelos de implementación de Cloud Computing.

Nubes públicas o externas

Las nubes públicas son hosteadas, operadas y manejadas por terceros desde uno o más Data Centers. Los servicios son ofrecidos a múltiples clientes sobre una infraestructura compartida.



En una nube pública, la gestión de la seguridad y las operaciones del día a día recaen en los proveedores del servicio. Por lo tanto, el cliente tiene un bajo grado de control y supervisión de los aspectos de seguridad física y lógica de una nube púbica.

Nubes privadas o internas

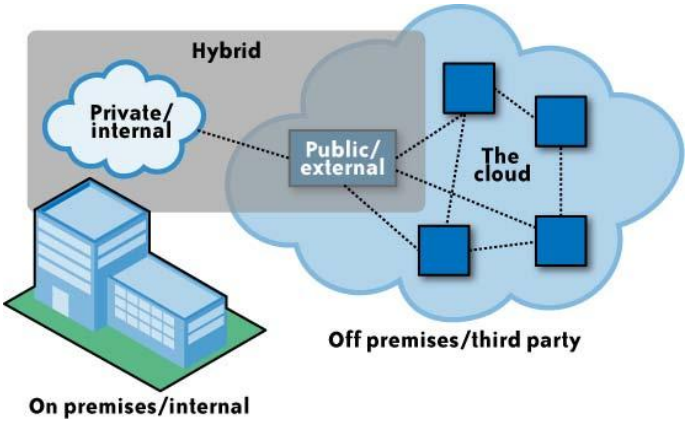
En las nubes privadas la infraestructura de red, cómputo y almacenamiento está dedicada a una sola organización y no es compartida con ninguna otra. Solo es accesible desde la red privada.

La organización tiene el control sobre la infraestructura lo que favorece la seguridad de los datos, el gobierno corporativo y la confiabilidad. Sin embargo, no se capitalizan los beneficios del pay-as-you-go ya que se debe pagar el costo de la infraestructura total para soportar los picos de uso del sistema.

En virtud de este modelo de gobierno directo, un cliente de una nube privada tiene un alto grado de control y supervisión sobre los aspectos lógicos y físicos de la seguridad de la infraestructura, tanto del hypervisor como de los sistemas operativos virtualizados. Debido a esto, es más fácil para el cliente cumplir con los estándares de seguridad establecidos por la empresa, con las políticas y regulaciones.

Nubes híbridas

Las nubes híbridas son una combinación de las públicas y las privadas, donde los datos y aplicaciones críticas se mantienen en la nube privada mientras que el resto en la pública.



Nubes de comunidad

La infraestructura del cloud es compartida por varias organizaciones y soporta una comunidad específica con intereses comunes (objetivos, requerimientos de seguridad, regulaciones, etc). Puede ser manejada por las organizaciones o por terceros.

Seguridad en Cloud Computing

Los controles de seguridad para Cloud Computing son en general similares a los aplicados en otros ambientes de IT. Sin embargo los riesgos presentes pueden ser diferentes debido a las tecnologías involucradas y a los modelos de servicio y de despliegue.

Los controles se implementan en las distintas capas del modelo de servicio, que abarcan la seguridad física, la seguridad de red, del sistema y de las aplicaciones. Dependiendo del modelo de servicio varían las responsabilidades de seguridad que tienen el cliente y el proveedor. En el modelo SaaS el cliente sólo es responsable de utilizar la aplicación en forma segura, mientras que el proveedor es quien debe garantizar la seguridad desde la capa física hasta la de aplicación. En cambio, en el modelo IaaS, el proveedor asegura desde la capa física hasta el hypervisor, dejándole al usuario la responsabilidad de las capas superiores.

Beneficios de seguridad

A continuación se presentarán los principales beneficios de seguridad que ofrece el modelo de Cloud Computing.

Seguridad y beneficios de escala

Las medidas de seguridad son más económicas cuando se implementan a gran escala. Entonces, la misma inversión en seguridad permite comprar una mejor protección. Esto incluye una variedad de defensas como filtros, manejo de parches, instancias de máquinas virtuales e hypervisores reforzados, recursos humanos y su gestión, redundancia de hardware y software, mecanismos de autenticación fuertes, entre otras. Otros beneficios de escala son:

- Los proveedores de Cloud Computing tienen generalmente los recursos económicos para replicar contenido en distintas ubicaciones incrementando la redundancia, lo que permite una mayor tolerancia y recuperación ante fallas.
- La posibilidad de almacenar, procesar y entregar los datos más cerca de los extremos de la red incrementa la confiabilidad y la calidad del servicio, y reduce la propagación de los problemas de red.
- Se tiene mayor capacidad para responder a incidentes en forma eficaz y eficiente.
- Los proveedores de Cloud Computing pueden afrontar el costo de contratar personal altamente capacitado para tratar cuestiones de seguridad específicas.

Seguridad como un diferencial en el mercado

La seguridad es una prioridad para muchos de los clientes de Cloud Computing. La reputación en relación a cuestiones de confidencialidad, integridad, tolerancia a fallas y los servicios de seguridad ofrecidos hacen la diferencia al momento de elegir un proveedor. Esto incentiva a los proveedores a competir para brindar mejor seguridad.

Interfaz estándar para servicios de gestión de seguridad

Los servicios de gestión de seguridad (MSS) incluyen asesoramiento, respuesta a incidentes, manejo del perímetro remoto, monitoreo y penetration tests periódicos.

Los proveedores de Cloud Computing pueden ofrecer una interfaz abierta y estandarizada a los proveedores de MSS que les dan servicio a sus clientes, facilitando y reduciendo los costos de cambiar de proveedor de MSS.

Escalamiento de recursos

Entre los recursos que se pueden escalar rápidamente y por demanda se encuentran el almacenamiento, los ciclos de CPU, la memoria, los requerimientos de servicio web e instancias de máquinas virtuales.

Un proveedor de Cloud Computing tiene la capacidad de reasignar recursos dinámicamente, permitiendo dedicar más recursos a soportar medidas defensivas, como control de tráfico, filtros o mecanismos de cifrado, en el momento en que se produce o es probable que ocurra un ataque. Si esto se combina con métodos apropiados de optimización de recursos, el proveedor de Cloud Computing puede ser capaz de limitar el efecto que algunos ataques provocan en la disponibilidad de los recursos utilizados por los servicios legítimos, como así también limitar el efecto de asignar más recursos a los mecanismos defensivos en el momento de un ataque.

Auditoría y recolección de evidencia

El modelo de Cloud Computing soporta la clonación de imágenes u otros componentes virtuales para realizar un análisis forense fuera de línea en caso de que se sospeche que la seguridad fue comprometida, lo que permite disminuir el tiempo en que el sistema está fuera de servicio para realizar el análisis.

Pueden crearse múltiples copias y paralelizar las actividades de análisis para reducir el tiempo de investigación, lo que aumenta la probabilidad de rastrear a los atacantes y posibilita corregir antes las vulnerabilidades, llevando a un menor tiempo de exposición.

A su vez, el modelo provee un almacenamiento más flexible y rentable, lo que permite guardar logs más compresibles sin comprometer la performance y simplifica la realización de ajustes para satisfacer los requerimientos de logs de auditoría futuros. Esto hace más eficiente el proceso de identificación de los incidentes de seguridad a medida que ocurren.

Updates y defaults

Las imágenes de máquinas virtuales y los módulos de software usados por los clientes pueden estar previamente reforzados, configurados y actualizados para mejorar la seguridad. También es posible crear imágenes de la infraestructura virtual y compararlas regularmente con un patrón para detectar irregularidades (por ejemplo, para asegurar que las reglas del firewall no han cambiado). Además, contar con una plataforma homogénea permite desplegar las actualizaciones con mayor rapidez, reduciendo el tiempo de exposición. En el caso de los modelos SaaS y PaaS, es probable que las aplicaciones hayan sido reforzadas para ejecutarse fuera del entorno empresarial, haciéndolas más robustas que sus equivalentes en el modelo de software tradicional.

Auditorías y SLAs obligan a un mejor manejo de riesgos

La necesidad de cuantificar las penalidades para varios escenarios de riesgo en SLAs (acuerdos de nivel de servicio) y el posible impacto de las brechas de seguridad en la reputación, motiva a desarrollar procedimientos internos de auditoría y evaluación de riesgos más rigurosos. Además, las frecuentes auditorías impuestas sobre los proveedores de Cloud Computing tienden a exponer

riesgos que de otra manera podrían no haber sido descubiertos, con la consecuente mejora en la seguridad.

Beneficios de concentración de recursos

Aunque tiene desventajas obvias, la concentración de recursos facilita el establecimiento de un perímetro y el control del acceso físico a los recursos. También hace más sencilla y económica la aplicación de procedimientos relacionados con la seguridad como el control sobre el manejo de datos, actualizaciones, mantenimiento e incidentes.

Riesgos de seguridad

A continuación se describen los principales riesgos que se presentan en el modelo de Cloud Computing.

Pérdida de gobierno

En el uso de infraestructuras cloud, el cliente cede necesariamente al proveedor un número de cuestiones que pueden afectar la seguridad. Por ejemplo, el proveedor le puede impedir al usuario que realice escaneo de puertos, evaluación de vulnerabilidades y penetration testing.

Los acuerdos de nivel de servicio (SLA) pueden no obligar al proveedor a proporcionar el nivel de seguridad requerido por el cliente, dejando una brecha en las defensas de seguridad. Otra cuestión que lleva a la pérdida de gobierno ocurre cuando los terceros contratados por el proveedor influyen en la seguridad de cliente y no brindan las mismas garantías que el proveedor.

La pérdida de gobierno y control podría comprometer los requerimientos de seguridad, la confidencialidad, integridad y disponibilidad de datos, y causar un deterioro del rendimiento y calidad del servicio. Esto conlleva un impacto considerable sobre la estrategia de la organización y, por consiguiente, en la capacidad para cumplir con sus objetivos.

VULNERABILIDADES
ROLES Y RESPONSABILIDADES POCO CLAROS
CUMPLIMIENTO DEFICIENTE DE LAS DEFINICIONES DE LOS ROLES
ATRIBUCIÓN ERRÓNEA DE RESPONSABILIDADES AL PROVEEDOR
AUDITORÍAS O CERTIFICACIONES NO DISPONIBLES POR PARTE DEL PROVEEDOR
DEPENDENCIA DEL PROVEEDOR HACIA TERCEROS
FALTA DE SOLUCIONES Y TECNOLOGÍAS ESTANDARIZADAS
FALTA DE INFORMACIÓN SOBRE LA UBICACIÓN DE DATOS
RESTRICCIONES EN LOS PROCESOS DE EVALUACIÓN DE VULNERABILIDADES
FALTA DE CLARIDAD O COMPLETITUD DE LOS TÉRMINOS DE USO

Lock-In

Si la portabilidad de los datos y servicios es baja, es difícil para el cliente cambiar de proveedor o volver a un ambiente de cómputo tradicional, lo que introduce una dependencia del cliente hacia el proveedor. Si el proveedor quiebra y el costo de realizar la migración de las aplicaciones y el contenido a otro entorno es muy grande, o no se dispone del tiempo suficiente para realizarla, el cliente se vería seriamente afectado.

La adquisición del proveedor de Cloud Computing por parte de otra firma puede tener un efecto similar, debido al posible cambio en las políticas de servicio y las condiciones que no estén reguladas en contratos.

Los proveedores pueden tener un incentivo para no ofrecer buena portabilidad, aunque ofrecerla también podría significar una ventaja competitiva.

El lock-in puede manifestarse de diferentes maneras de acuerdo al modelo de servicio de Cloud Computing en cuestión:

- En el modelo SaaS, los datos de los clientes suelen estar almacenados en un esquema de base de datos que varía de proveedor a proveedor. Generalmente se dispone de funciones en la API que permiten leer registros de datos. Con esas funciones, en caso que el proveedor no ofrezca facilidades adicionales de exportación de datos, el cliente necesitará crear sus propias rutinas de exportación, que lean y transformen sus datos a una representación adecuada para importarlos a otro entorno. El cliente podría pagarle al proveedor nuevo para asistirlo en esta tarea.
  El cambio de proveedor también impacta en los usuarios finales de las aplicaciones SaaS, que pueden tener que ser recapacitados, con el consecuente costo para el cliente, especialmente si los usuarios son numerosos. Además, si se contaba con programas que interactuaban directamente con la API del proveedor anterior, por ejemplo para integrar diferentes aplicaciones, los mismos deberán ser reescritos para adecuarlos a la API nueva.
- En el modelo PaaS, los clientes desarrollan sus aplicaciones basándose en la API que les ofrece el proveedor. El lock-in se da a nivel de la API, debido a que la misma generalmente varía de proveedor a proveedor. También pueden existir diferencias en los soportes de runtime, modificados y configurados para operar en forma segura en un entorno cloud, quedando a cargo del cliente entender y tomar en cuenta estas diferencias. En el modelo PaaS, al igual que en el SaaS, se puede dar el lock-in a nivel de datos, pero en este caso, es el cliente el responsable de crear las facilidades de exportación de datos apropiadas.
- En el modelo IaaS, el lock-in puede deberse a la incompatibilidad en las tecnologías de virtualización o a la falta de portabilidad de datos.

VULNERABILIDADES
FALTA DE SOLUCIONES Y TECNOLOGÍAS ESTANDARIZADAS
ELECCIÓN INADECUADA DEL PROVEEDOR
FALTA DE CLARIDAD O COMPLETITUD DE LOS TÉRMINOS DE USO

Falla de aislamiento

La abstracción de recursos físicos compartidos en recursos lógicos dedicados mediante virtualización, es una característica fundamental del Cloud Computing. Esta clase de riesgo consiste en la falla de los mecanismos de separación de recursos entre los diferentes usuarios de la infraestructura compartida.

Los ataques al hypervisor y las inyecciones SQL que exponen datos de múltiples clientes son algunos de los ataques que pueden originar fallas de aislamiento.

La probabilidad de ocurrencia de estos incidentes depende del modelo de despliegue en cuestión, siendo menor en el caso de las nubes privadas que en las públicas.

Las consecuencias de una falla de aislamiento pueden incluir pérdida de datos críticos, daños en la reputación e interrupción del servicio tanto de los proveedores de Cloud Computing como de los clientes.

VULNERABILIDADES
VULNERABILIDADES EN EL HYPERVISOR
FALLA EN EL AISLAMIENTO DE LOS RECURSOS
IMPACTO DE ACTIVIDADES DE UN CLIENTE EN LA REPUTACIÓN DE OTRO
CHEQUEOS ILEGALES DE RED Y RESIDENCIA

Problemas de cumplimiento

Algunas organizaciones pueden haber realizado importantes inversiones para obtener determinada certificación, ya sea para lograr una ventaja competitiva o para cumplir con una regulación o estándar de la industria. Estas inversiones pueden verse en riesgo al migrar a la nube si el proveedor de Cloud Computing no es capaz de ofrecer evidencia de que cumple con los requerimientos relevantes o si no permite auditorías por parte del cliente.

Algunas certificaciones no pueden alcanzarse utilizando una infraestructura de nube pública, debiendo emplearse otras alternativas para brindar servicios que necesiten dichas certificaciones.

VULNERABILIDADES
AUDITORÍAS O CERTIFICACIONES NO DISPONIBLES POR PARTE DEL PROVEEDOR
FALTA DE SOLUCIONES Y TECNOLOGÍAS ESTANDARIZADAS
FALTA DE INFORMACIÓN SOBRE LA UBICACIÓN DE DATOS
FALTA DE CLARIDAD O COMPLETITUD DE LOS TÉRMINOS DE USO

Interfaz de administración comprometida

Las interfaces de administración en las nubes públicas son accesibles a través de Internet y permiten controlar más cantidad de recursos que en los ambientes de cómputo tradicionales, por lo que suponen un mayor riesgo, especialmente si se combinan con vulnerabilidades en los browsers y en el acceso remoto. Esto hace necesario utilizar mecanismos de autenticación fuertes, por ejemplo autenticación de dos factores.

Pueden verse afectadas tanto las interfaces de los clientes que controlan cierto número de máquinas virtuales, como las de los proveedores que controlan el sistema completo.

VULNERABILIDADES
VULNERABILIDADES AAA (AUTHENTICATION, AUTHORIZATION AND ACCOUNTING)
ACCESO REMOTO DESDE PUNTOS INSEGUROS
ERRORES DE CONFIGURACIÓN
VULNERABILIDADES EN LOS SISTEMAS OPERATIVOS
VULNERABILIDADES EN LAS APLICACIONES Y MANEJO INADECUADO DE ACTUALIZACIONES

Intercepción y filtrado de datos

Al tratarse de un sistema distribuido, en el modelo de Cloud Computing existe un mayor tráfico de datos que en el sistema tradicional, debido a que se tiene una mayor transferencia de datos entre la infraestructura Cloud y los clientes remotos.

Se deben tener en cuenta ataques como sniffing, spoofing, man-in-the-middle, canales ocultos, replay, entre otros.

Además, en algunos casos los SLAs no ofrecen cláusulas de confidencialidad para garantizar la protección de la información del cliente y no especifican cómo circularán los datos dentro de la nube.

VULNERABILIDADES
VULNERABILIDADES AAA (AUTHENTICATION, AUTHORIZATION AND ACCOUNTING)
VULNERABILIDADES EN LA ENCRIPTACIÓN DE DATOS
CHEQUEOS ILEGALES DE RED Y RESIDENCIA
FALTA DE CLARIDAD O COMPLETITUD DE LOS TÉRMINOS DE USO
VULNERABILIDADES EN LAS APLICACIONES Y MANEJO INADECUADO DE ACTUALIZACIONES
BORRADO DE DATOS INSEGURO

Atacante interno

Las actividades de un atacante interno pueden impactar sobre la confidencialidad, integridad y disponibilidad de los datos, los servicios, y por lo tanto, en la reputación de la organización. Esto se puede considerar especialmente importante en el caso de Cloud Computing debido a que estas arquitecturas necesitan ciertos roles que suponen un riesgo muy alto (ejemplo: administrador de sistemas del proveedor).

VULNERABILIDADES
ROLES Y RESPONSABILIDADES POCO CLAROS
CUMPLIMIENTO DEFICIENTE DE LAS DEFINICIONES DE LOS ROLES
PRINCIPIO DE NEED-TO-KNOW NO APLICADO
VULNERABILIDADES AAA (AUTHENTICATION, AUTHORIZATION AND ACCOUNTING)
VULNERABILIDADES EN LOS SISTEMAS OPERATIVOS
PROCEDIMIENTOS DE SEGURIDAD FÍSICA INADECUADOS
VULNERABILIDADES EN LAS APLICACIONES Y MANEJO INADECUADO DE ACTUALIZACIONES

Otros riesgos

Distributed denial of service: se puede lleva a cabo generando un gran flujo de información desde varios puntos de conexión. La forma más común de realizar un DDoS es a través de una botnet.

Economic denial of service: los recursos de un cliente de cloud son usados por un atacante y causan un impacto económico en el cliente. Por ejemplo, robo de identidad, el proveedor no limita el uso de los recursos pagos, un atacante utiliza un canal público a fin de agotar los recursos limitados del cliente, etc.

Pérdidas de claves de cifrado: esto involucra la revelación de las claves secretas (SSL, cifrado de archivos, claves de los clientes particulares, etc) a terceros maliciosos, la pérdida o corrupción de las llaves, o su uso no autorizado para la autenticación y no repudio (firma digital).

Ataques de ingeniería social: las vulnerabilidades explotadas por los atacantes pueden ser la falta de concientización sobre la seguridad, vulnerabilidades en el cifrado de las comunicaciones, procedimientos inadecuados de seguridad física, etc.

Logs comprometidos: incluye tanto a los logs operacionales como a los de seguridad.

Vulnerabilidades

A continuación se detallan las principales vulnerabilidades nombradas anteriormente que dan lugar a los riesgos mencionados anteriormente. Algunas de ellas son específicas del modelo de Cloud Computing mientras que otras también están presentes en el modelo de cómputo tradicional.

Roles y responsabilidades poco claros

Esta vulnerabilidad consiste en la especificación inadecuada de los roles y responsabilidades dentro de la estructura del proveedor de Cloud Computing.

Cumplimiento deficiente de las definiciones de los roles

Una falla en la separación de los roles en el proveedor de Cloud Computing puede dar lugar a roles excesivamente privilegiados, haciendo el sistema vulnerable. Por ejemplo, una sola persona no debería poder acceder a la nube entera.

Principio de need-to-know no aplicado

Consiste en que en la definición de roles y responsabilidades se otorguen mayores privilegios de los que se necesitan para desarrollar las tareas encomendadas.

Atribución errónea de responsabilidades al proveedor

Los clientes de Cloud Computing pueden no estar al tanto de las responsabilidades que tienen asignadas en los términos de servicio y atribuirlas erróneamente al proveedor. Por ejemplo, el cliente podría considerar que el proveedor debe encriptar sus archivos, aún cuando no está especificado en el contrato.

Falta de información sobre la ubicación de datos

Almacenar los datos en mirrors para utilizarlos en redes periféricas o guardarlos en forma redundante sin que el cliente disponga de información de su ubicación en tiempo real introduce cierto grado de vulnerabilidad.

Vulnerabilidades en el hypervisor

Los ataques a la capa del hypervisor son muy atractivos ya que en esta capa se controlan los recursos físicos y las máquinas virtuales que están corriendo en el sistema. Una vulnerabilidad en esta capa es entonces crítica debido a que explotarla significa potencialmente explotar cada máquina virtual.

Algunos escenarios de ataque al hypervisor son el guest to host escape y el VM-hopping. Este último consiste en hackear una máquina virtual y, explotando alguna vulnerabilidad en el hypervisor, tomar control de otras máquinas virtuales ejecutándose en el mismo hypervisor.

Falla en el aislamiento de los recursos

El uso de recursos por parte de un cliente puede afectar la utilización de recursos de otro. En el modelo de Cloud Computing los recursos físicos son compartidos por múltiples máquinas virtuales y por lo tanto por múltiples clientes. Las vulnerabilidades en el hypervisor pueden llevar al acceso no autorizado de estos recursos compartidos. Esto podría ocurrir si por ejemplo las máquinas virtuales de dos clientes tienen sus discos virtuales almacenados en la misma LUN (logic unit number) de un SAN y uno de ellos logra mapear el disco virtual del otro en su máquina virtual obteniendo los permisos para ver y utilizar sus datos.

En el modelo IaaS el proveedor brinda a sus clientes una interfaz para gestionar sus recursos. Una vulnerabilidad en esta interfaz puede permitir el acceso no autorizado a los recursos del cliente, posibilitándole al atacante provocar denial of service, compromiso y fuga de datos, o daños financieros.

Chequeos ilegales de red y residencia

Un cliente puede llevar a cabo distintos tipos de pruebas sobre otros clientes dentro de la red interna, por ejemplo el escaneo de puertos. También puede realizar chequeos de residencia para determinar qué recursos comparten los distintos clientes.

Vulnerabilidades AAA (authentication, authorization and accounting)

Un sistema pobre de autentificación, autorización y de registros de auditoría y contabilidad puede facilitar el acceso a recursos no autorizado, el escalado de privilegios y hacer difícil la tarea de rastrear el uso ilegal de recursos y los incidentes de seguridad en general.

Algunas vulnerabilidades específicas de este tipo son:

- Almacenamiento inseguro de las credenciales de acceso a la nube por parte del cliente
- Roles insuficientes
- Credenciales almacenadas en máquinas transitorias

El modelo de Cloud Computing hace que los ataques a mecanismos de autentificación basados en password tengan mayor impacto ya que las aplicaciones de la empresa están expuestas a internet. Esto hace necesaria la utilización de mecanismos de autentificación fuertes como por ejemplo autentificación de dos factores.

Vulnerabilidades en la encriptación de datos

Estas vulnerabilidades consisten en la posibilidad de leer datos en tránsito utilizando ataques como man-in-the-middle, explotando mecanismos de autentificación pobres o aceptando certificados firmados por entidades inválidas.

Se incluyen además en esta clase de vulnerabilidades las fallas en la encriptación de los datos almacenados en archivos, bases de datos, imágenes de maquinas virtuales no montadas, datos e imágenes forenses, logs críticos, entre otros.

Borrado de datos inseguro

Cada vez que un cliente cambie de proveedor, los recursos se reduzcan o el hardware se reubique, entre otros casos, los datos pueden quedar disponibles más allá del tiempo de vida especificado en la política de seguridad. Podría ser imposible llevar a cabo los procedimientos especificados por la política de seguridad, ya que la eliminación completa de todos los datos sólo es posible mediante la destrucción de un disco que también almacena los datos de otros clientes.

Además, las APIs ofrecidas por el proveedor pueden no soportar procedimientos de borrado seguro de datos.

El cifrado de los datos en el disco reduce considerablemente la posibilidad de explotar esta vulnerabilidad.

Conclusión

En este informe se presentó el concepto de Cloud Computing como un mecanismo para adquirir tecnologías de información como servicio, junto a sus principales características, modelos de servicio y de despliegue. Sobre esta definición se trataron los diferentes aspectos en relación a la seguridad, considerando los principales beneficios y riesgos.

En el modelo de Cloud Computing la organización le cede al proveedor el control de un número cuestiones que hacen a la seguridad del sistema. Esto resulta beneficioso si la organización no cuenta con la capacidad de manejar la seguridad en forma adecuada ya que se la deja en manos de terceros, aprovechando así las ventajas del modelo de Cloud Computing entre las que se destacan la economía de escala, la seguridad como diferencial en el mercado y la resistencia de los sistemas ante ataques. Sin embargo, las organizaciones que sí son capaces de garantizar el nivel de seguridad que desean, pueden inclinarse por los ambientes de cómputo tradicionales para evitar exponerse a los riesgos propios del modelo de Cloud Computing, como la pérdida de gobierno, el lock-in o las fallas de aislamiento.

Cuando se considera adoptar el modelo de Cloud Computing es necesario evaluar los riesgos y beneficios que ofrece y compararlos con los presentes en el sistema actual.

Por lo tanto, cuando se considera adoptar el modelo de Cloud Computing es necesario evaluar los riesgos y beneficios que ofrece y compararlos con los presentes en el sistema actual.

Referencias

- Cloud Security and Privacy – Oreilly
- Cloud Computing Security Risk Assessment - ENISA
- Cloud Security Alliance
- Cloud Computing Security - iSEC Partners