Published on *Revista .Seguridad* (https://revista.seguridad.unam.mx)

TIPS DE SEGURIDAD PARA EL CÓMPUTO EN NUBE

Anaid Guevara Soriano
José Reinel Ramirez Solares

consejos

numero-08

Hoy en día se escucha hablar mucho del término cloud computing, que en español se interpretaría como “cómputo en la nube”, éste parece ser novedoso, sin embargo, muchas de sus aplicaciones se utilizan diariamente sin darse cuenta, por ejemplo en: las redes P2P, muchos servicios gratuitos de Google, el proyecto SETI@Home, ciertos servicios web curiosos, e incluso algunos sistemas operativos como Jolicloud. Estos sistemas se gestionan en la nube y el usuario final tan sólo se conecta utilizando la potencia de los servidores sin necesidad de tener éstos consigo. A veces es necesario un pequeño programa cliente, hecho a medida. Pero en la mayoría de las ocasiones basta tan sólo un navegador web.

Un grupo de expertos del NIST (National Institute of Standards and Technology) realizó un estudio sobre los principales problemas de seguridad que aún hay que superar para poder aplicar esta tecnología a un nivel mucho más amplio. Pero existen diversas opiniones de primer nivel que ven problemas mucho más serios, asociados a la privacidad y a la libertad del usuario.

La estructura del sistema permite el acceso a un grande y poderosos equipo de cómputo sin necesidad de mantenimiento por parte del usuario. Esto hace que sea una plataforma ideal para el desarrollo de proyectos científicos que necesitan computadoras de gran potencia y que de otra manera no podrían tener acceso a ellas. Sobre este modelo de funcionamiento también se soportan sistemas de gestión internos de empresas, como Opentaps, así como un modelo de negocio dirigido a ellas. Proveedores

de servicios en la nube son Sun, IBM, Amazon y Google entre otros. Y entre sus clientes hay grandes empresas, como General Electric.

El modelo de servicios del entorno de computación en nube está comprendido por tres opciones centrales (Fig. 1):

• El software como Servicio (SaaS). Comprende aplicaciones para usuarios finales entregadas como servicios, en lugar de software en-premisa.
• La plataforma como Servicio (PaaS). Provee una plataforma para aplicaciones o middleware como un servicio en el que los desarrolladores pueden crear y desplegar aplicaciones personalizadas.
• La infraestructura como Servicio (IaaS). Concierne el hardware, la tecnología para el almacenamiento, funcionamiento de sistemas operativos e informáticos; otras infraestructuras entregadas como fuera-de-premisas, servicios bajo demanda en vez de dedicados y recursos en el sitio, tales como el Amazon Elastic Compute Cloud (Amazon EC2) o el Amazon Simple Storage Service (Amazon S3).

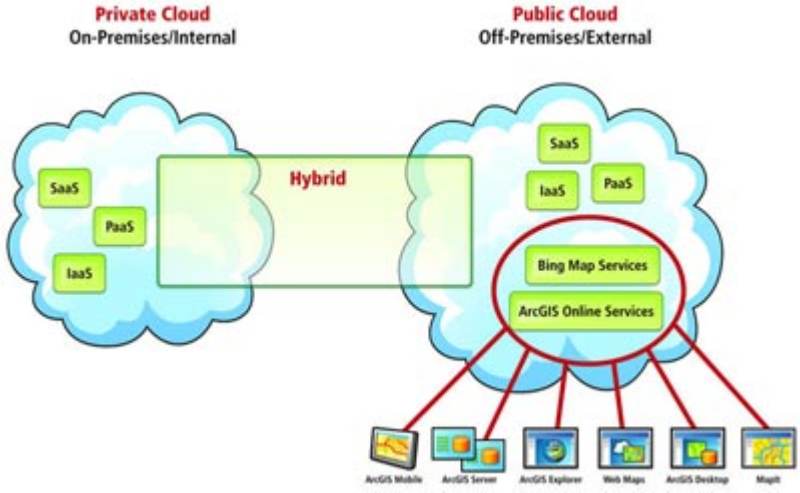

Fig. 1

A pesar de ello, cabe destacar que si bien es cierto que el cloud computingtrae consigo grandes ventajas, también es cierto que cuanta más crítica es la aplicación más importante es la fiabilidad del sistema, así como la seguridad de los datos. Por consiguiente, se tiene una mayor susceptibilidad a ser víctima de un ataque con fines maliciosos.

A continuación se enuncian algunos de los tips respecto a las medidas esenciales de seguridad que se deben considerar para poder hacer uso de la nube de manera segura, evitando así la mayoría de los riesgos que esto implica:

1. CONSIDERAR LA GUÍA DE LA ALIANZA DE SEGURIDAD EN CÓMPUTO REFERENTE A LA NUBE.

Los puntos más destacados de esta guía son:

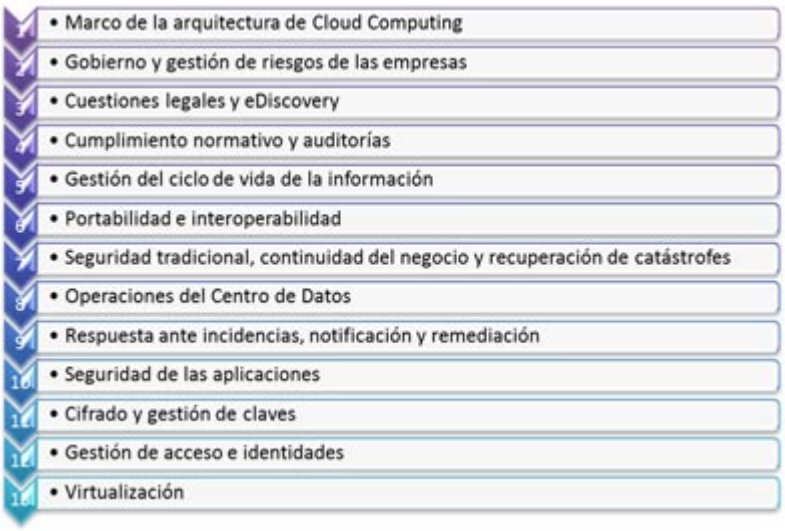

Fig. 2

Para una lectura a detalle de cada uno, sugerimos dirigirse a:
http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

2. ELEGIR ADECUADAMENTE LA CONTRASEÑA

Otro asunto preocupante de los servicios del cómputo en la nube es que, a pesar de las medidas de protección que implementan todas las empresas, la seguridad de las cuentas de los usuarios depende de la contraseña asignada a cada una de éstas.

Un ejemplo de las consecuencias dadas por utilizar contraseñas inseguras fue evidente hace poco en el caso Twittergate, en el que un cracker obtuvo numerosos documentos corporativos pertenecientes al popular servicio de microblogging, Twitter, y los publicó en el sitio de noticias y tecnologíaTechCrunch.

Estos documentos estaban alojados en Google Docs y a pesar de que Googleno puede aceptar la responsabilidad por la fuga de información, los archivos no hubieran sido robados en primer lugar si hubieran estado albergados detrás de un firewall. En lugar de eso, la información clave de la compañía estuvo a punto de ser descubierta, “a un password descifrado de distancia”.

La diferencia entre una red corporativa y una cuenta en línea es que en un ecosistema de negocios, los administradores pueden crear políticas para la creación de contraseñas que los obliguen a mantener ciertos niveles de complejidad y a crear nuevas contraseñas periódicamente. No obstante, en la nube, tenemos la libertad de establecer lo que sea como contraseña y no volver a cambiarla nunca más. Ésta es un área que aún necesita mucho trabajo. Por tal situación se recomienda:

1. Selección de contraseñas “fuertes”, difíciles de descifrar.
2. Mantenerlas en secreto.
3. No transferirlas.

4. No escribirlas en papeles de fácil acceso o en archivos sin cifrar.
5. No habilitar la opción “recordar clave en este equipo”, que ofrecen los programas.
6. No enviarlas por correo electrónico.
7. Cambiarlas frecuentemente.

3. CIFRAR DATOS EN LA NUBE

Otra de las debilidades (poco conocidas) de cómputo en la nube es que pocas máquinas tienen acceso a los números generados al azar que se necesitan para cifrar información.

Los detalles de este lío son excesivamente técnicos pero el resultado es que la inherente naturaleza de la computación virtual hace mucho más simple la tarea a los hackers y crackers porque les permite adivinar con facilidad los números utilizados para generar las llaves de cifrado.

Si bien éste no es un problema inmediato que atenta contra la integridad de la nube, sí requerirá investigación a largo plazo.

Para el cifrado de datos en la nube se recomienda:

1. Administración remota segura. Cifrado del tráfico.
2. Clasificar y cifrar información sensible con aplicaciones de cifrado confiables.
3. Utilizar tecnologías de cifrado de punto a punto (VPN).

4. USAR ADECUADAMENTE LOS SERVICIOS DE LA NUBE

Si consideramos los problemas ya descritos, probablemente pensaremos dos veces antes de confiar en los servicios que funcionan a través de la nube.

Pero, ¿En verdad es tan malo? ¿Es la nube una plataforma peor de lo que ya tenemos?

En realidad, a pesar de que la nube traerá bajo el brazo un paquete de retos y amenazas con las que estaremos lidiando en el futuro inmediato, esto será precisamente durante las primeras fases de la transición. Tampoco presenta amenazas necesariamente peores que las del sistema tradicional.

Al final de cuentas, el mercado como ente regulador y espontáneo hará que los desarrolladores y propietarios de servicios para la nube hagan propuestas cada vez más sólidas y seguras. Serán justamente esas personas las mejor recompensadas por sus esfuerzos y, sus plataformas, las que adoptarán los usuarios.

Los servicios que funcionan a través de la nube no son como deberían ser actualmente, pero en poco tiempo podrán competir fácilmente con cualquier otra plataforma. En efecto, podría llegar el día donde sean consideradas incluso más seguras. Hasta entonces, los usuarios deben proceder con precaución cuando se muden a la nube. Al menos, deben hacerlo conscientes de las capacidades y los riesgos

que ello implica.

5. PRECISAR INFORMACIÓN A COMPARTIR Y POR COMPARTIR

1. Clasificar la información sensible y separarla de la información publica.
2. Crear cuentas de acceso a la información pública con mínimos privilegios.

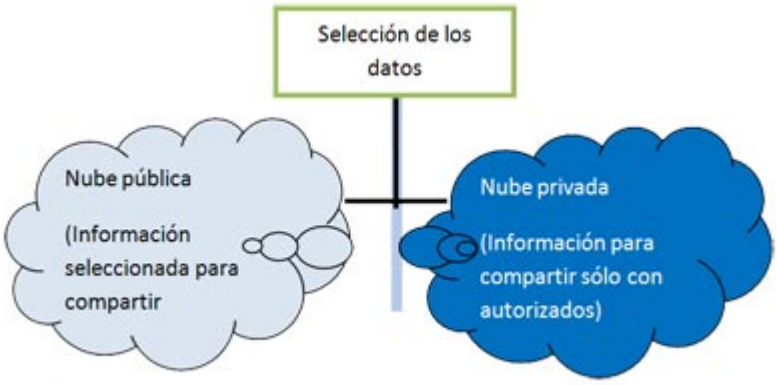

Fig. 3

6. APLICAR “MEJORES PRÁCTICAS” DE SEGURIDAD AL MOMENTO DE CONFIGURAR LAS APLICACIONES

Es necesario que los usuarios incorporen buenas prácticas para proteger el entorno de información y prevenir aún más la posibilidad de formar parte del conjunto que engloba a potenciales y eventuales víctimas de cualquiera de las amenazas, quienes constantemente buscan sacar provecho de las debilidades humanas. Para ello se obligatorio conocer los peligros latentes y la forma de detenerlos a través de mecanismos de prevención.

1. Cambiar usuarios y contraseñas por default.
2. Cambiar periódicamente la contraseña de administración.
3. Quitar servicios y cuentas no utilizados.
4. Actualizar frecuentemente sus aplicaciones con los “parches de seguridad”.
5. Copias de Seguridad de los archivos de configuración de las aplicaciones.
6. Descargar las aplicaciones y actualizaciones de sitios confiables.

7. REGISTRAR DE MANERA EXHAUSTIVA EL ENTORNO PARA DETECTAR ACTIVIDADES O CAMBIOS NO SOLICITADOS YA SEA EN PROCESOS, TAREAS O DOCUMENTOS

1. Monitoreo de servicios críticos.

2. Utilización de herramientas que buscan y detectan problemas de seguridad; localizan intrusos y controlan cambios.
3. Análisis periódico de logs (bitácoras).
4. Crear respaldos de configuraciones.
5. Utilizar antivirus y anti-spyware.

8. APLICAR CONFORME A LO DISPUESTO POR EL PROVEEDOR DE SERVICIOS, PARCHES Y CORRECCIÓN DE VULNERABILIDADES.

1. Descargar las aplicaciones y actualizaciones de sitios confiables del proveedor.
2. Aplicar parches en ambiente de prueba antes de aplicarlos a los servidores de producción.
3. Elaborar y mantener respaldos de su información personal o de datos críticos, de lo contrario, si algo le pasa al sistema no podrá recuperar su trabajo.

9. ESTABLECER DE FORMA REGULAR UN ANÁLISIS DE VULNERABILIDADES Y AUDITORÍAS DE LA CONFIGURACIÓN

Realizar auditorías y análisis de vulnerabilidades permitirá identificar debilidades en aquellos puntos susceptibles a algún ataque malicioso, los cuales pueden propiciar diversos daños, por ejemplo atentar contra la confidencialidad, integridad y disponibilidad de los datos concentrados en dicha nube.

Referencias:

- CLOUD SECURITY ALLIANCE (CSA). “Top Threats to Cloud Computing V1.0”, marzo 2010, auspiciada por HP, 14 PP. (en)http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
- http://www.rsa.com/innovation/docs/CLWD_BRF_1009.pdf
- http://www.maestrosdelweb.com/editorial/amenazas-seguridad
- http://www.tendencias21.net/Problemas-de-seguridad-en-la-nube_a3381.html
- http://www.bsecure.com.mx/en-linea/the-cloud-reloaded-seguridad-en-la-nube/
