VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Noviembre 2016

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

Usando la nube de forma segura

Resumen

“La nube” puede significar diferentes cosas para distintas personas, pero por lo general es usar un servicio a través de Internet para almacenar y administrar tus sistemas de computación y/o datos. Una ventaja de la nube es que puedes acceder y sincronizar fácilmente los datos desde múltiples dispositivos en cualquier parte del mundo, y también puedes compartir tu información con cualquier persona que quieras. Llamamos a estos servicios “la nube” porque a menudo no sabes dónde se almacenan físicamente tus datos. Ejemplos de cómputo en la nube incluyen la creación de documentos en Google Docs, compartir archivos vía Dropbox, la creación de un propio servidor en la nube de Amazon, almacenamiento de datos de los clientes en Salesforce o archivar música o fotos en iCloud de Apple. Estos servicios en línea pueden hacerte mucho más productivo, pero también conllevan riesgos únicos. En este boletín te decimos cómo puedes hacer uso de la nube de forma segura.

Editor Invitado

Dave Shackleford (**@daveshackleford**) es un consultor profesional, dueño de Voodoo Security y autor de numerosos cursos de formación del SANS, incluyendo SANS Security 579: Virtualización y Seguridad de una Nube Privada y Security 524: Fundamentos de Seguridad en la Nube.

Elige un proveedor de servicios en la nube

La nube no es ni buena ni mala, es una herramienta para hacer las cosas tanto en la oficina como en el hogar. Sin embargo, cuando utilizas estos servicios estás entregando tus datos privados a otros esperando que los mantengan seguros y disponibles a la vez. Por lo anterior, debes estar seguro de haber elegido bien a tu proveedor de servicios en la nube. Para tus computadoras de trabajo y la información relacionada con el lugar donde laboras, consulta con tu supervisor para ver si tu compañía te permite utilizar los servicios en la nube. Si está permitido el uso de la nube, confirma cuáles servicios puedes utilizar y cuáles son las políticas sobre el uso de ellos. Si estás considerando un servicio para tu uso personal, debes tomar en cuenta lo siguiente:

1. **Soporte**. ¿Qué tan fácil es conseguir ayuda o tener respuesta a una pregunta? ¿Hay una dirección de correo electrónico donde puedas ponerte en contacto, foros públicos donde puedas enviar tus dudas o existe un apartado de preguntas frecuentes en su sitio web?
2. **Simplicidad**. ¿Qué tan fácil es usar el servicio? Cuanto más complejo es el servicio, es más probable que cometas

Usando la nube de forma segura

errores y accidentalmente expongas o pierdas tu información. Selecciona un proveedor en nube que encuentres fácil de entender, configurar y utilizar.

3. **Seguridad**. ¿Qué datos recopila acerca de ti? ¿Cómo se transfieren los datos desde tu computadora a la nube y cómo se almacenan en esta? ¿Cifran los datos?, y si es así, ¿quién puede descifrarlos?
4. **Términos de servicio**. Toma un momento para revisar los términos del servicio (sorprendentemente, a menudo son fáciles de leer). Confirma quién puede acceder a tus datos y cuáles son tus derechos legales, así como las responsabilidades asumidas por el proveedor.

La nube puede hacer que tu información sea más accesible y aumentar tu productividad, pero ten cuidado en cómo accedes y compartes tu información.

Asegura tus datos

Una vez que elegiste tu proveedor de servicios en la nube, el siguiente paso es asegurarte de utilizar los servicios apropiadamente. La forma en la que accedes y compartes tus datos a menudo puede tener un impacto mucho mayor en la seguridad de tus archivos que cualquier otra cosa. Estos son algunas cuestiones que debes tomar en cuenta:

1. **Autenticación**: Utiliza una fuerte y única contraseña para autenticar tu cuenta. Si tu proveedor ofrece la verificación en dos pasos es muy recomendable que lo habilites. Este es uno de los pasos más importantes que puedes seguir para proteger tu cuenta.
2. **Compartir archivos/carpetas**: La nube hace que sea muy fácil compartir, a veces es demasiado simple. En el peor caso, puedes pensar que estás compartiendo tus archivos con solo una persona, pero podrías accidentalmente hacer que tus archivos o incluso carpetas estén disponibles públicamente para todos en Internet. La mejor forma de protegerte es no compartir alguno de tus archivos por defecto, solo permite que personas específicas (o grupos de personas) accedan a archivos específicos o carpetas. Cuando alguien ya no necesita acceder a tus archivos, remuévelos. Tu proveedor debe proporcionarte una forma sencilla para realizar el seguimiento de quién tiene acceso a los archivos y carpetas.
3. **Compartir archivos/carpetas usando enlaces**: Una función común de algunos servicios en la nube es la posibilidad de crear un enlace que dirige a tus archivos o carpetas. Esta característica te permite compartir estos archivos con cualquier persona que quieras, simplemente proporcionando un enlace web. Sin embargo, se tiene muy poca seguridad. Cualquiera que conozca este enlace puede tener acceso a tus archivos o carpetas personales. Si

Usando la nube de forma segura

envías el enlace a una sola persona, esta podría compartir el enlace con otros o aparecer en los motores de búsqueda. Si compartes los datos mediante el uso de un vínculo, asegúrate de deshabilitar el enlace una vez que ya no sea necesario, establece una fecha de caducidad o, si es posible, protege el enlace con una contraseña.

4. **Ajustes**: Entiende las configuraciones de seguridad que ofrece tu proveedor de nube. Por ejemplo, si compartes una carpeta con alguien más, ¿puede compartir tus datos con terceros sin tu conocimiento? También puedes saber quién ha visto tu contenido compartido y cuándo lo vieron. ¿Puedes compartir restringiendo a "solo lectura" en vez de otorgar el permiso de "lectura y escritura", el cual significa que las personas pueden además modificar los archivos?
5. **Antivirus**: Asegúrate que la última versión del software antivirus esté instalado en tu computadora y cualquier otro equipo que utilices para compartir tus datos. Si un archivo que estás compartiendo se infecta, las otras computadoras que accedan al mismo archivo también podrían infectarse.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: securingthehuman.sans.org/ouch/archives

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Recursos

Seguridad para el cómputo en nube:	http://revista.seguridad.unam.mx/numero-08/tips-de-seguridad-para-el-computo-en-nube
Privacidad de la información en la nube:	http://revista.seguridad.unam.mx/numero-08/privacidad-informacion-nube
Contraseñas seguras:	https://revista.seguridad.unam.mx/numero-15/guia-para-contrasenas-seguras
Cómputo en nube, ventajas y desventajas:	http://revista.seguridad.unam.mx/numero-08/computo-nube-ventajas-desventajas
Perspectivas sobre el uso de la nube:	http://revista.seguridad.unam.mx/numero-08/todo-depende-cristal-mire-nube
Seguridad en la nube para una IES:	http://revista.seguridad.unam.mx/numero27/seguridad-en-la-nube-para-una-ies

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Leticia González y Katia Rodríguez

