VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Septiembre 2014

Boletin mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Información general
- Selección de un proveedor de la nube
- Protección de tus datos

El uso seguro de la nube

Información general

“La nube” es una poderosa tecnología que tanto las personas como las organizaciones están adoptando rápidamente. “Nube” puede significar diferentes cosas para diferentes personas pero generalmente se refiere a la utilización de un proveedor de servicios en Internet para almacenar y gestionar datos. Una ventaja de la nube es que, además de acceder fácilmente y sincronizar tu información desde múltiples dispositivos en cualquier parte del mundo, también puedes compartirla con quien lo desees. La razón por la que llamamos “la nube” a estos servicios es que a menudo no se sabe dónde se almacenan físicamente los datos. Ejemplos de computación en la nube incluyen la creación de documentos en Google Drive, el compartir archivos a través de Dropbox, la creación de tu propio servidor en la nube de Amazon o el almacenamiento de tu música y fotos en iCloud de Apple. Estos servicios en línea tienen el potencial de incrementar en gran medida tu productividad, sin embargo, también presentan riesgos únicos. En este boletín abordaremos cómo aprovechar de forma segura la nube.

Editor Invitado

James y Kelli Tarala (**@isaudit** **@kellitarala**) son los consultores principales de Enclave Security y autores de numerosos cursos de formación del SANS que incluyen SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls (Auditoría 566: Implementación y Auditoría de Veinte Controles de Seguridad Críticos) y MGT 415: A Practical Introduction to Risk Assessments (MGT 415: Una Introducción Práctica a las Evaluaciones de Riesgo).

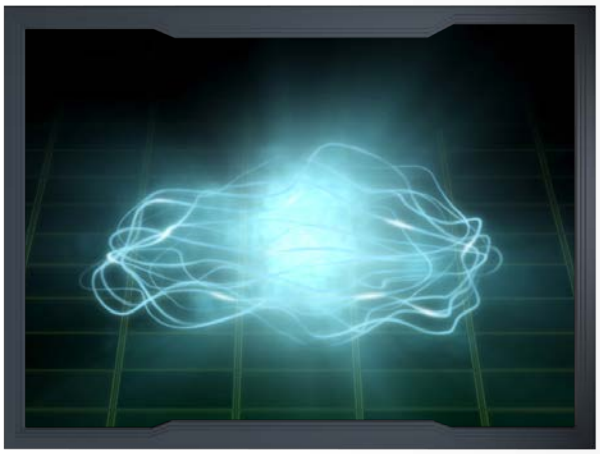
Selección de un proveedor de la nube

La nube no es buena o mala, es una herramienta para hacer cosas, tanto en el trabajo como en el hogar. Al utilizar estos servicios, estás entregando tu información personal a desconocidos, por lo que esperas es que estén protegidos y, al mismo tiempo, disponibles. Por ello, debes estar seguro de elegir sabiamente. Para equipos de trabajo e información relacionada con el trabajo, consulta a tu supervisor para saber si puedes usar los servicios de la nube. Si está permitido su uso, por favor asegúrate de confirmar qué servicios puedes usar y cuáles son las políticas sobre la forma de utilizarlos. Si estás considerando un servicio de nube para tu uso personal, ten en cuenta lo siguiente:

1. **Apoyo**: ¿Es fácil conseguir ayuda o respuesta a tus preguntas? ¿Hay un número telefónico al que puedas llamar o una dirección de correo electrónico para ponerte en contacto? ¿Existen otras opciones de apoyo, tales como foros públicos o preguntas frecuentes en su sitio web?
2. **Simplicidad**: ¿Qué tan fácil es usar el servicio? Entre más complejo sea el servicio, más probable es que cometas errores y tu información quede expuesta accidentalmente. Usa un proveedor de nube que te resulte fácil de entender, configurar y utilizar.

El uso seguro de la nube

3. **Seguridad**: ¿De qué forma llegan los datos desde tu computadora a la nube?, ¿es segura la conexión mediante cifrado?, ¿de qué forma están almacenados los datos?, ¿están cifrados? y si es así, ¿quién puede descifrarlos?
4. **Términos del servicio**: Tómate un momento para revisar los Términos de Servicio (que a menudo son sorprendentemente fáciles de leer). Confirma quién puede acceder a tus datos y cuáles son tus derechos legales.



La nube puede hacer que tu información sea más accesible y ayudarte a ser más productivo, pero ten cuidado de cómo almacenar y compartir esa información.

Protección de tus datos

Una vez que hayas seleccionado un servicio de nube, el siguiente paso consiste en asegurarse de que lo utilizas correctamente. La forma en que accedes y compartes tus datos a menudo puede tener un impacto en la seguridad de tus archivos mucho mayor que cualquier otra cosa. Algunos pasos clave que puedes seguir incluyen:

1. **Autenticación**: Usa una contraseña fuerte y única para autenticarte en tu cuenta. Si tu proveedor de nube ofrece verificación de dos pasos es muy recomendable que lo habilites.
2. **Compartir archivos/carpetas**: La nube hace que sea muy fácil compartir, a veces demasiado. En el peor de los casos, es posible que accidentalmente hagas públicos tus archivos o incluso carpetas enteras en todo Internet. La mejor manera de protegerte es configurar tu cuenta para que de forma predeterminada no compartas los archivos, de esta forma sólo permitirás a personas específicas (o grupos de personas) el acceso a archivos o carpetas con base en quién necesita tener acceso. Cuando alguien ya no tenga acceso a tus archivos, elimínalo. Tu proveedor de nube debe proporcionar una manera sencilla de realizar el seguimiento de quién tiene acceso a tus archivos y carpetas.
3. **Compartir archivos/carpetas usando enlaces**: Una característica común de algunos servicios de la nube es la capacidad de crear un enlace de Internet que dirija a los archivos o carpetas. Esta característica te permite compartir estos archivos con quien quieras simplemente proporcionando el enlace web. Sin embargo, este enfoque tiene muy poca seguridad ya que cualquier persona que conozca este enlace puede tener acceso a tus archivos personales o carpetas. Si envías el enlace a una sola persona, esa persona podría compartir ese enlace con otros o incluso podría aparecer en motores de búsqueda. Si compartes los datos mediante el uso de un vínculo, asegúrate de deshabilitarlo una vez que ya no sea necesario, si es posible, protégelo con una contraseña.
4. **Ajustes**: Es importante comprender las configuraciones de seguridad ofrecidas por el proveedor de nube. Por

El uso seguro de la nube

ejemplo, si compartes una carpeta con otra persona, puede que a su vez ésta comparta tus datos con otros sin tu conocimiento.

5. **Antivirus**: Asegúrate de tener instalada la última versión del software antivirus en tu computadora y en cualquier otro equipo utilizado para compartir tus datos. Si un archivo que estás compartiendo se infecta, otras computadoras que accedan a ese mismo archivo también podrían infectarse.
6. **Copia de seguridad**: Aunque tu proveedor de nube esté respaldando tus datos, considera la posibilidad de hacer copias de seguridad por tu cuenta. Esto no sólo protege tus datos en caso de que tu proveedor de nube vaya a la quiebra o por alguna razón cierre tu cuenta y se vuelva inaccesible, sino que puede ser mucho más fácil recuperar grandes cantidades de datos desde la copia de seguridad local que bajándolos de la nube. Asimismo, confirma la frecuencia con la que tu proveedor de nube realiza copias de seguridad de tus archivos, si te permiten recuperar versiones anteriores de tus archivos y cuánto tiempo mantiene las copias de seguridad disponibles.

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: http://www.securingthehuman.org

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

Contraseñas seguras:	http://www.securingthehuman.org/ouch/2013#may2013
Administradores de contraseñas:	http://www.securingthehuman.org/ouch/2013#october2013
Copias de seguridad:	http://www.securingthehuman.org/ouch/2013#september2013
Condiciones de seguridad:	http://www.securingthehuman.org/resources/security-términos

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Kristian Araujo

