VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Agosto 2015

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Qué y cuándo respaldar
- Cómo respaldar
- Recuperación
- Puntos clave

Respaldos y recuperación

Resumen

Es posible que tarde o temprano algo salga mal y pierdas tus archivos personales, documentos o fotos. Por ejemplo, que borres por accidente los archivos incorrectos, suceda alguna falla de hardware, pierdas tu laptop o tu computadora se infecte. En momentos como éste los respaldos son la única manera de reconstruir tu vida digital. En este boletín te explicamos qué son los respaldos, cómo respaldar tu información y cómo desarrollar la estrategia adecuada para ti.

Editor Invitado

Heather Mahalik es una experta reconocida en la industria de forense, quien se enfoca principalmente en análisis forense a smartphones. Es coautora de Practical Mobile Forensics, editora técnica de Learning Android Forensics y de FOR585 Advanced Smartphone Forensics y FOR518 Macintosh Forensics del Instituto SANS. Sigue a Heather en **Smarterforesnics.com** y en su Twitter **@heathermahalik**.

Qué y cuándo respaldar

Los respaldos son copias de seguridad de tu información que almacenas en algún otro lugar. Cuando pierdes información importante para ti puedes recuperar los datos desde tus respaldos. El problema es que mucha gente no realiza copias de seguridad, lo que es una pena porque pueden ser fáciles de realizar y económicas. Hay dos enfoques para decidir qué respaldar: (1) datos específicos que son importantes para ti; o (2) todo, incluyendo el sistema operativo completo. El primer enfoque simplifica las copias de seguridad y ahorra espacio en el disco duro, sin embargo, el segundo enfoque es más simple y más completo. Si no estás seguro de qué respaldar, entonces se recomienda hacer copias de seguridad de todo.

Tu siguiente decisión será sobre la frecuencia con la que respaldarás tus datos. Las opciones más comunes son cada hora, día, semana, etc. Para uso en casa, los programas personales como Time Machine de Apple o Windows Backup and Restore de Microsoft te permite programar respaldos automáticos para que los configures y te olvides de ellos. Estas soluciones respaldan tu información de manera silenciosa durante el día mientras haces uso o no de tu computadora. Otra soluciones ofrecen “protección continua” en la que archivos nuevos o modificados son respaldados inmediatamente al momento de cerrarlos. Te recomendamos, por lo menos, respaldar diariamente. Al final, la pregunta que deberías hacerte es: “¿Cuánta información estoy dispuesto a perder si tengo que realizar una restauración desde una copia de seguridad?”.

Cómo respaldar

Existen dos maneras de respaldar tus datos: en medios físicos o en almacenamiento en la nube. Los medios físicos son cualquier tipo de hardware, como DVDs, memorias USB o discos duros externos. En cualquier medio que elijas, recuerda nunca respaldar tus archivos en el mismo dispositivo que contiene los archivos originales. El problema con el

Respaldos y recuperación

almacenamiento en medios físicos es que si su ubicación sufre algún desastre (como fuego o robo) entonces no sólo perderás tu computadora sino también tus respaldos. Por ello, debes tener un plan para alojar las copias de tus respaldos en otra ubicación segura. Si así lo haces, etiquétalos indicando qué y cuándo se respaldó. Para mayor seguridad cifra tus respaldos.

Los respaldos fiables y automatizados son la última línea de defensa en la protección de tus datos.

Las soluciones en la nube son diferentes, este es un servicio en el que tus archivos son almacenados en algún lugar de Internet. Dependiendo de cuántos datos desees respaldar éste puede ser un servicio de pago. Estas funcionan instalando un programa en tu computadora que automáticamente respalda tus archivos por ti. La ventaja con esta solución es que desde el momento en que tus respaldos están en la nube, si sucede un desastre en tu casa, tus respaldos estarán a salvo. Asimismo, puedes acceder a ellos desde casi cualquier lugar hasta cuando viajas. La desventaja es que los respaldos en la nube (y la recuperación) puede ser lenta, especialmente si tienes una gran cantidad de datos. Si no estás seguro de que tipo de respaldo es el mejor para ti (medios físicos o en la nube) ten en cuenta que puedes realizar ambos.

Por último, no olvides tus dispositivos móviles. La ventaja con éstos es que la mayoría de tus datos están almacenados en la nube, como tu correo, calendario y contactos. De cualquier manera, seguramente tienes información que no está almacenada en la nube como las configuraciones de tus aplicaciones, fotos recientes o preferencias del sistema. Al respaldar tu dispositivo móvil no sólo preservas la información, sino que también es más fácil restaurarlo, como por ejemplo, cuando cambias de equipo y transfieres tu información. Un iPhone o una iPad puede respaldarse automáticamente con iCloud de Apple; los dispositivos Android u otros dependen de su fabricante o proveedor de servicio. En algunos casos deberás comprar alguna aplicación móvil diseñada en específico para realizar respaldos.

Recuperación

Respaldar tu información es sólo la mitad de la batalla, debes tener la certeza que puedes recuperarla. Verifica cada mes que tus respaldos funcionan recuperando un archivo y validando su contenido. También, asegúrate de realizar un respaldo de todo el sistema antes de una actualización mayor (como transferir a una computadora o a un dispositivo móvil nuevo) o una reparación mayor (como reemplazar un disco duro) y verifica que sea restaurable.

Respaldos y recuperación

Puntos clave

- Automatiza tus respaldos tanto como te sea posible y verifícalos regularmente.
- Cuando restaures un sistema entero desde un respaldo, asegúrate de aplicar nuevamente los últimos parches y actualizaciones antes de usarlo de nuevo.
- Copias de seguridad desactualizadas u obsoletas pueden convertirse en un riesgo y deben ser destruidos para prevenir que sean accedidos por usuarios no autorizados.
- Si utilizas una solución en la nube, investiga las políticas y reputación del proveedor y cerciórate que cumpla con tus requerimientos. Por ejemplo, ¿cifra tus datos cuando son almacenados? ¿Quién tienen acceso a tus respaldos? ¿Cuenta con autenticación fuerte como la verificación en dos pasos?

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

Verificación en dos pasos:	http://www.securingthehuman.org/ouch/2013#august2013
Seguridad en la nube:	http://www.securingthehuman.org/ouch/2014#september2014
Cifrado:	http://www.securingthehuman.org/ouch/2014#august2014
Consejos:	http://www.seguridad.unam.mx/usuario-casero/consejos/

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Célica Martínez Aponte

