Boletín mensual de concientización en seguridad para ti

¿Realizo respaldos?

Resumen

Si utilizas una computadora o un dispositivo móvil, tarde o temprano, algo saldrá mal. Accidentalmente puedes borrar los archivos equivocados, presentarse una falla en el hardware o perder el dispositivo. Peor aún, un malware como ransomware puede borrar tus archivos y/o mantenerlos cautivos. En momentos como estos, los respaldos son la única manera en la que puedes reconstruir tu vida digital.

Qué, cuándo y cómo

Los respaldos son copias de tu información almacenadas en un lugar diferente a tu computadora o dispositivo móvil. Cuando pierdes datos valiosos, puedes recuperar tus datos de los respaldos. El primer paso es decidir qué es lo que vas a respaldar, (1) datos específicos que son importantes para ti o (2) todo, incluyendo el sistema operativo. Muchas soluciones de respaldos están configuradas de forma predeterminada para utilizar el primer enfoque, estas respaldan las carpetas más utilizadas. Si no estás seguro sobre qué respaldar o quieres ser más cuidadoso, respalda todo.

Segundo, decide la periodicidad con la que respaldarás tu información. Los programas para realizar respaldos que ya se encuentran en los sistemas operativos como Time Machine de Apple o Backup and Restore de Windows te permiten “configurar y olvidar” una programación automática de respaldos. Las opciones comunes incluyen cada hora, día, semana, etc. Otras soluciones ofrecen una “protección continua” en la que los archivos nuevos o modificados se copian inmediatamente cada vez que guardas un documento. Como mínimo, recomendamos realizar respaldos diarios automáticos de archivos críticos.

Finalmente, decide cómo vas a respaldar. Existen dos maneras: almacenamiento local o en la nube. Los respaldos locales dependen de los dispositivos que tu controlas como una memoria USB o dispositivos de red con acceso a Wi-Fi. La ventaja de estos respaldos es que te permiten respaldar y recuperar grandes cantidades de datos rápidamente. La desventaja, si te infectas con malware, como ransomware, es posible que la infección se propague a tus respaldos. Asimismo, si te ves envuelto en un desastre, como un incendio o robo, puede resultar que pierdas no solo tu computadora sino también los respaldos. Si utilizas dispositivos externos de respaldos, almacena una copia en otro lugar seguro (fuera del sitio donde están tus dispositivos) y verifica que tus respaldos estén correctamente etiquetados.

Las soluciones basadas en la nube son servicios en línea que almacenan tus archivos en Internet. Por lo general, instalas una aplicación en tu computadora, esta respalda automáticamente tus archivos de forma programada o a medida que

los modificas. Una ventaja de las soluciones en la nube es su simplicidad, los respaldos suelen ser automáticos y puedes acceder a tus archivos desde cualquier lugar. Además, debido a que tus datos residen en la nube, los desastres domésticos como incendios o robos no afectarán tu respaldo. Finalmente, los respaldos en la nube pueden ayudarte a recuperarte de infecciones de malware, como el ransomware. La desventaja depende de la capacidad para respaldar y restaurar la cantidad de datos respaldados y de la velocidad de la red. ¿No estás seguro si deseas utilizar respaldos locales o en la nube? Refuerza tu seguridad y utiliza ambos.

Con los dispositivos móviles muchos de tus datos ya están almacenados en la nube. Sin embargo, las configuraciones de tus aplicaciones móviles, fotos recientes y preferencias del sistema no lo están. Al hacer una copia de seguridad de tu dispositivo, no solo conservas esta información, sino que también es más fácil transferir tus datos cuando cambias a un nuevo dispositivo.

Puntos clave

- **Respaldar tus datos es solo la mitad de la batalla, debes estar seguro de poder recuperarlo. Prueba periódicamente que tus respaldos funcionan recuperando y abriendo un archivo.**
- **Si reconstruyes un sistema a partir de un respaldo, asegúrate de aplicar los últimos parches y actualizaciones de seguridad antes de volver a utilizarlo.**
- **Si utilizas una solución en la nube, selecciona una que sea fácil de utilizar e investiga las opciones de seguridad. Por ejemplo, si soporta la verificación de dos factores para asegurar tu cuenta en línea.**

Los respaldos son una manera simple y económica de proteger tu vida digital.

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

Editor Invitado

Matt Bromiley *es profesional en ciberseguridad y respuesta a incidentes, ha trabajado con organizaciones de diferentes tamaños. También es instructor del SANS, imparte clases avanzadas de respuesta a incidentes y threat hunting, en los cursos de FOR508 y FOR572. Puedes encontrarlo en Twitter como* @mbromileyDFIR.

Recursos

Creando contraseñas simples:	https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Spanish_0.pdf
Evita el malware:	https://www.sans.org/sites/default/files/2018-06/201806-OUCH-June-Spanish.pdf
Creando un hogar ciberseguro:	https://www.sans.org/sites/default/files/2018-01/201801-OUCH-January-Spanish_0.pdf