El Boletín Mensual de Concientización en Seguridad para ti

¿Tienes respaldos?

Resumen

Si usas una computadora o un dispositivo móvil durante el tiempo suficiente, tarde o temprano algo saldrá mal. Puedes eliminar accidentalmente los archivos incorrectos, tener una falla de hardware o perder un dispositivo. Peor aún, tus archivos pueden ser infectados por malware, borrados y cifrados. En momentos como estos, los respaldos suelen ser la única forma en que puedes reconstruir tu vida digital.

Los respaldos son copias de seguridad de tu información almacenada en otro lugar que no sea tu computadora o dispositivo móvil. Cuando pierdas o no puedas acceder a datos valiosos en tu dispositivo, puedes recuperarlos desde las copias de seguridad. Muchos de los archivos que creamos actualmente ya se almacenan y respaldan automáticamente en la nube, como documentos de Microsoft Word almacenados en Microsoft OneDrive, Dropbox o Google Drive, o fotos personales almacenadas en Apple iCloud. Pero puede haber archivos que no se guarden automáticamente en la nube; o tal vez deseas copias de seguridad adicionales para uso personal.

Qué, cuándo y dónde

El primer paso es decidir qué deseas respaldar: (1) solo datos específicos que son importantes para ti; o (2) todo, quizás incluyendo el sistema operativo completo. Muchas soluciones de respaldo están configuradas de manera predeterminada para usar el primer enfoque y solo respaldan las carpetas más utilizadas. Si no estás seguro de qué respaldar o quieres ser más cuidadoso, considera hacer una copia de seguridad de todo.

El segundo paso es decidir con qué frecuencia respaldar los datos. El software de respaldos integrado en tu sistema, como Time Machine de Apple o Windows Backup and Restore, permiten generar un programa calendarizado para configurarlo una vez y olvidarte de esta labor. Las opciones de programación comunes incluyen respaldo por hora, por día y por semana. Otras soluciones pueden ofrecer "protección continua" en la que los archivos se respaldan inmediatamente a medida que se editan o guardan. Como mínimo, recomendamos copias de seguridad diarias automatizadas de archivos críticos.
Finalmente, decide cómo vas a realizar la copia de seguridad. Hay dos formas: respaldos locales o en la nube. Las copias de seguridad locales se basan en dispositivos que controlas físicamente, como unidades USB externas o dispositivos accesibles en red. La ventaja de las copias de seguridad locales es que te permiten crear respaldos y recuperar grandes cantidades de datos rápidamente. La desventaja es que si te infectas con malware, es posible que la infección se propague a tus copias de seguridad. Además, si sufres un desastre, como un incendio o un robo, podrías perder tanto las copias de seguridad como tu computadora.
Si usas dispositivos externos para las copias de seguridad, guarda una copia fuera del sitio en un lugar distinto que sea seguro y verifica que los respaldos estén debidamente etiquetados. Para mayor seguridad, considera cifrar dichas copias de seguridad.

Las soluciones en la nube son servicios en línea que respaldan y almacenan sus archivos en Internet. Por lo general, te pedirán instalar una aplicación en tu computadora. Luego, la aplicación realiza una copia de seguridad automática de sus archivos, ya sea en un horario definido o a medida que los modifica o guarda. Algunas ventajas de las soluciones en la nube son su simplicidad, la automatización de las copias de seguridad y el acceso a los archivos desde casi cualquier lugar. Además, dado que tus datos residen en la nube, los desastres domésticos, como incendios o robos, no afectarán tu copia de seguridad. La principal desventaja es el ancho de banda que consume. La capacidad para realizar copias de seguridad y restaurar depende de la cantidad de datos que estés respaldando y de la velocidad de su red. ¿No estás seguro si quieres usar copias de seguridad locales o en la nube? Ten mayor seguridad y usa ambos.

Con los dispositivos móviles, la mayoría de tus datos, como correos electrónicos, mensajes de texto o fotos que toma, se almacenan automáticamente en la nube. Sin embargo, es posible que las configuraciones de tus aplicaciones móviles, las preferencias del sistema y otros archivos no se almacenen en la nube. Al hacer una copia de seguridad automática de tu dispositivo móvil, no solo conservas esta información, sino que es más fácil transferir tus datos cuando actualizas a un nuevo dispositivo.

Puntos clave adicionales

- Comprueba periódicamente que tus copias de seguridad funcionan recuperando y abriendo un archivo.
- Si reconstruyes un sistema a partir de un respaldo, incluido el sistema operativo, asegúrate de volver a aplicar los últimos parches y actualizaciones de seguridad antes de volver a utilizarlo.
- Si estás utilizando una solución en la nube, selecciona una que te resulte fácil de usar e investiga las opciones de seguridad. Por ejemplo, ¿tu proveedor de respaldos en la nube admite la verificación en dos pasos para proteger tu cuenta en línea?

Las copias de seguridad son una forma sencilla y económica de proteger tu vida digital.

Editor invitado

Greg Scheidel es CISO en Iron Vine Security, con más de 30 años de experiencia en tecnologías de información y seguridad. También es instructor del instituto SANS, en donde enseña arquitectura de seguridad, ingeniería y zero trust en el curso SEC530. Puedes encontrarlo en Twitter @greg_scheidel.

Recursos

Doble factor de autenticación: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Usando la nube de forma segura: https://www.sans.org/newsletters/ouch/securely-using-the-cloud/
Gestores de contraseñas: https://www.sans.org/newsletters/ouch/password-managers/
Herencia digital: https://www.sans.org/newsletters/ouch/digital-inheritance/

Traducido para la comunidad por: Célica Martínez Aponte and Iván Galindo, UNAM-CERT