Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

Entendiendo el cifrado

EDITOR INVITADO

Fred Kerby es el editor invitado para este número de OUCH! Recientemente se retiró de la Naval Surface Warfare Center Dahlgren Division donde se desempeñó durante los últimos 16 años como Director de Seguridad de la Información. Fred es instructor senior de SANS Institute.

¿Qué es el cifrado?

El cifrado es un mecanismo que protege tu información importante, como documentos, fotografías o transacciones en línea, del acceso o modificación por personas no autorizadas. El cifrado funciona utilizando un “algoritmo” (fórmula matemática) y una llave, para convertir datos legibles (texto plano) a una forma que otros no puedan entender (texto cifrado). El algoritmo es la receta general para el cifrado y tu llave hace únicos los datos cifrados – sólo personas con tu llave única y el mismo algoritmo pueden descifrarlo. Las llaves generalmente son una larga secuencia de números protegidos por un mecanismo común de autenticación como contraseñas, tokens o biométricos, como tu huella digital.

CIFRA TU INFORMACIÓN ALMACENADA

Información sensible como, por ejemplo, información médica, financiera o de negocios, puede almacenarse en tus dispositivos móviles como tu laptop, memoria USB, smartphone o tableta. Estos dispositivos son fáciles de robar o perder y, si no están cifrados, el contenido puede ser leído por cualquiera que tenga acceso a ellos. Una de las mejores formas para proteger los datos en un dispositivo móvil es cifrándolos.

En general, existen tres formas de cifrar datos almacenados en tus dispositivos móviles. Puedes cifrar archivos específicos, carpetas completas e incluso todo el disco duro. La mayoría de los sistemas operativos soportan al menos una opción, si no es que todas. El cifrado completo del disco, comúnmente llamado Full Disk Encryption (FDE) se considera lo más seguro. FDE cifra todos los datos en tu disco duro, incluyendo cualquier archivo temporal. Esto también simplifica el proceso de decidir qué cifrar y qué no cifrar. Si no puedes cifrar por completo el disco duro, cifra algún archivo o carpeta que contenga información sensible.

Los dispositivos móviles, como memorias USB, pueden venir con la capacidad de cifrado incorporada o puedes cifrarlas instalando software adicional en tu computadora. Los smartphones y tablets también pueden contar con su propia capacidad de cifrado, o bien, puedes instalar aplicaciones de cifrado –consulta la tienda de aplicaciones del fabricante para obtener información acerca de lo que está disponible.

Entendiendo el cifrado

CIFRA LA INFORMACIÓN QUE ENVÍES

La información también es vulnerable al momento de enviarse. Si los datos no están cifrados, pueden ser monitoreados y capturados en línea. Por ello, debes asegurarte que cualquier comunicación sensible esté cifrada, tal como, banca en línea, envío de correos electrónicos o incluso cada vez que accedes a tu cuenta de Facebook. La forma más común de cifrado en línea es HTTPS o conexiones seguras a sitios web. Esto significa que el tráfico entre tu navegador y el sitio web está cifrado. Busca **https://** en la URL o el icono del candado en tu navegador. Muchos sitios soportan esto por defecto (como Google Apps), y sitios como Facebook y Twitter ofrecen la opción de configurar tu cuenta para forzar el uso de HTTPS. Adicionalmente, cuando te conectes a una red Wi-Fi pública, procura utilizar siempre una red cifrada. Actualmente, WPA2 es uno de los mecanismos de cifrado más fuertes y hasta el momento el más recomendable. Finalmente, siempre que envíes o recibas correos electrónicos, asegúrate que el cliente de correo esté configurado para utilizar canales cifrados. Unos de los más usados es SSL (Secure Socket Layer). Muchos clientes de correo utilizan SSL por defecto.

El cifrado es una herramienta importante para la protección de datos, pero sólo es efectiva si tienes contraseñas fuertes y mantienes la seguridad completa de tu computadora.

MEJORES PRÁCTICAS Y SUGERENCIAS

Sin importar el tipo de cifrado que utilices o la manera en la que lo hagas, casi todas las formas de cifrado comparten algunas características sobre las que debes estar consciente.

- Tu cifrado es sólo tan fuerte como los son tus llaves. Si tu llave está comprometida, también lo están tus datos. Si estás utilizando contraseñas para proteger tus llaves, asegúrate de utilizar contraseñas fuertes y protegerlas bien. (Consulta la edición de mayo de 2011 del OUCH! sobre contraseñas).
- No pierdas tus llaves o el acceso a ellas. Si pierdes las llaves de cifrado o no puedes tener acceso a ellas porque has olvidado las contraseñas que las protegen, probablemente no puedas recuperar tus datos.
- Tu cifrado es tan fuerte como la seguridad de tu computadora. Si tu computadora está infectada, los intrusos pueden comprometer tu cifrado.
- Mantén la seguridad completa de tu computadora. El cifrado no funciona contra virus, gusanos, caballos de Troyanos, vulnerabilidades no parchadas o ataques de ingeniería social.

Entendiendo el cifrado

- Siempre asegúrate de respaldar cualquier dato confidencial de forma segura. Esto asegura que, si pierdes tu dispositivo o las llaves de cifrado que protegen tus datos, aún podrás recuperar tu información.

- Utiliza cifrado basado en algoritmos de dominio público como AES (Advanced Encryption Standard) o Blowfish, más que algoritmos propietarios. Además, siempre asegúrate de usar la última versión de tus programas de cifrado.

- Consulta a un profesional de TI si necesitas ayuda. La instalación, configuración o uso incorrecto del cifrado puede hacer que tu información quede permanentemente inaccesible.

RECURSOS

Algunos de los enlaces mostrados a continuación han sido reducidos para mayor legibilidad a través del servicio TinyURL. Para mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL, la cual muestra el destino del enlace solicitando permiso antes de ir a él.

Herramientas de cifrado de disco duro completo:
TrueCrypt: http://www.truecrypt.org/
PGP: http://www.pgp.com
Windows 7 Bitlocker: http://preview.tinyurl.com/3xaubbr

Cifrado de carpetas y archivos:
TrueCrypt: http://www.truecrypt.org/
Windows: http://preview.tinyurl.com/yb29rzn
Mac: http://preview.tinyurl.com/6c2q3cy

Cifrado USB:
TrueCrypt: http://www.truecrypt.org/
SanDisk: http://preview.tinyurl.com/3nl4g2p
IronKey: https://www.ironkey.com/products

Estándares de cifrado:
AES: http://preview.tinyurl.com/ku33x
WiFi: WPA y WPA2 http://preview.tinyurl.com/am5oa
Cómo trabaja HTTPS: http://preview.tinyurl.com/ya9se7f
Cómo trabaja una VPN: http://preview.tinyurl.com/rfc9f

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org.

VERSIÓN EN ESPAÑOL

UNAM-CERT, único equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país. Sitio web http://www.seguridad.unam.mx, síguelo en Twitter @unamcert.

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Versión en español a cargo de UNAM-CERT: Angie Aguilar, Miguel Mendoza, Galvy Cruz, Mauricio Andrade, Rubén Aquino