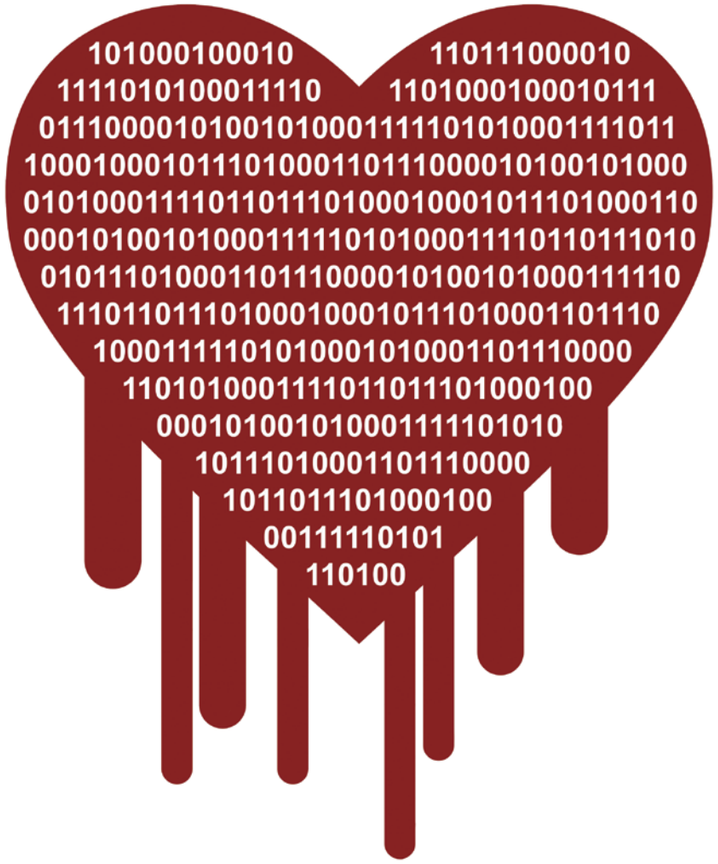
¿Qué hacer ante los fallos de seguridad en la Red?

El fallo Heartbleed ha puesto de manifiesto la importancia de utilizar contraseñas fuertes y únicas por cada sitio web



Un grupo de ingenieros localizó, a principios de abril, una vulnerabilidad en el código de OpenSSL, un software libre muy utilizado por sitios web de todo el mundo para cifrar datos sensibles de los usuarios, como contraseñas, nombres o correo electrónico. Empresas como Google, Facebook, Yahoo o PayPal, además de muchos bancos, lo usan para convertir en seguras las comunicaciones entre el usuario y el servidor de la página donde accede. Ahora, tras este fallo denominado Heartbleed, su seguridad ha quedado en entredicho. Ante este hecho, conviene conocer una serie de indicaciones acerca de cómo actuar ante Heartbleed y otros fallos de seguridad similares en la Red.

Un error global

El fallo Heartbleed ("corazón sangrante" en inglés) permite entrar en el inicio de sesión de otros usuarios gracias a unos pocos *kilobytes* de memoria (64kB) que el protocolo deja libres cuando se accede a un servidor seguro. Estos *bits* pueden ser utilizados para activar un programa de claves aleatorias que podría dar con las del usuario. Aun así, un atacante no puede elegir a qué sección de la memoria accede y, por lo tanto, que se asalte un servidor no significa que este vaya a darle con rapidez las contraseñas de las personas.

Al mismo tiempo que se anunciaba el fallo, también se publicó el parche para su solución, lo que llevó a muchas empresas a actualizar sus librerías de códigos. Sin embargo, se estima que cerca de un millón de servidores usaban alguna de las versiones de OpenSSL con este tipo de vulnerabilidad o *bug* descubierto. Algunas firmas de seguridad elevan la incidencia a una parte importante de Internet. De hecho, se considera que Heartbleed es uno de los tres mayores errores en la historia de la Red.

Lo más seguro: cambiar de clave

Uno de los problemas para los usuarios es que no pueden saber si sus datos han sido obtenidos de forma maliciosa por un tercero. Por lo tanto, la opción más segura es cambiar las contraseñas de todos los servicios que empleen OpenSSL.

Algunas plataformas de Internet han enviado correos electrónicos a sus usuarios donde se les avisa del fallo y se les recomienda el cambio de contraseña. Sin embargo, no todos los servicios han lanzado esta advertencia. Según Bloomberg, la NSA (Agencia Nacional de Inteligencia de EE.UU.) estuvo utilizando esta vulnerabilidad para acceder a información, aunque esto fue desmentido después por la propia NSA en Twitter.

Protegerse de Heartbleed

Hay algunas herramientas on line, como LastPass Heartbleed checker o Heartbleed test, que permiten averiguar si una página web es aún vulnerable a este fallo de seguridad. De esta forma, los usuarios pueden comprobar si sus datos personales están comprometidos. También existe una extensión para el navegador Chrome que avisa a la persona si accede a una página web vulnerable a Heartbleed.

Pero la recomendación más importante es cambiar la contraseña de los sitios que empleen OpenSSL y que hayan estado comprometidos. Como en la actualidad el usuario no puede saber cuáles lo fueron, el consejo se extiende a todos los servicios de la Red.

Contraseñas fuertes y únicas

Este importante fallo de seguridad ha puesto de manifiesto la importancia de contar con contraseñas fuertes y únicas por cada sitio web. Muchas personas usan la misma contraseña para darse de alta en decenas de páginas webs a través de Internet. Sin embargo, en el momento en que uno de estos servicios quede comprometido a través de un ataque malicioso que roba las credenciales de los usuarios, también se expondrá al mismo peligro al resto de sitios donde el ciudadano comparta la misma combinación de correo electrónico y nombre de usuario y contraseña.

Algunos consejos para elegir una contraseña pasan por buscar claves de más de ocho dígitos y que sean una combinación alfanumérica con signos de teclado. Para asegurarse de que la combinación es correcta, en Internet hay diferentes generadores de contraseñas fuertes.

Una regla mnemotécnica para crear contraseñas que puedan recordarse sin problemas consiste en pensar en una frase que el usuario pueda recordar con facilidad, seleccionar la inicial de cada palabra de la frase y poner algunas en mayúsculas, minúsculas y números para al final añadir algunos caracteres especiales. Así, para la frase "En un lugar de la mancha cuyo nombre no quiero acordarme", la contraseña podría ser "3EuldL1MCnNQA$".

Las contraseñas generadas no hay que dejarlas apuntadas en texto plano en un documento del ordenador, ya que un acceso no autorizado al dispositivo podría comprometer la seguridad del usuario. Para ello, existen algunas aplicaciones, como 1Password, LastPass o PassLocker, que almacenan y gestionan de forma segura las contraseñas de todos los servicios on line y aplicaciones del usuario.

Con todo, ni siquiera un cambio de contraseña a una más compleja y fuerte, nos hace totalmente inmunes a nuevos fallos causados por ciberdelincuentes. La mejor estrategia para prevenirlos es cambiar las claves con frecuencia y procurar no repetirlas. Así, podremos abortar un ataque que ya haya comenzado y obligar a los saboteadores de cuentas a iniciar de nuevo su trabajo. //