Descubren que los mensajes de WhatsApp pueden ser leídos

lunes, 23 de enero de 2017

El informe descubre una 'puerta de atrás' en la app. Así se puede evitar

Un experto descubre que el sistema puede generar nuevas claves de cifrado y acceder al contenido

Fue sin duda una de las medidas más importantes adoptadas por WhatsApp: incorporar un sistema de cifrado que hacía completamente inaccesible el contenido de una conversación salvo para los interlocutores. Mediante este sistema, el emisor genera -de una manera totalmente automatizada- unas claves que llegan el destinatario y sólo él puede descifrarlas. Este sistema de encriptación garantizaba la absoluta privacidad de las conversaciones, pero una investigación, desvelada por The Guardian, ha descubierto un agujero en este sistema que permitiría acceder al contenido de los mensajes.

En el Preguntas y Respuestas de WhatsApp podemos leer: “El cifrado de extremo a extremo en WhatsApp asegura que solo tú y el receptor puedan leer lo que se envía, y que nadie más, ni siquiera WhatsApp lo pueda hacer”. Una explicación rotunda y que no deja lugar a dudas, pero que ahora ha sido derribaba gracias a un estudio llevado a cabo por la Universidad de California. Su máximo responsable, el experto en seguridad Tobías Boelter, ha descubierto una puerta de atrás (backdoor) mediante la cual el sistema podría cambiar esas claves temporales y asignar unas nuevas que permitieran acceder al contenido.

El sistema podría cambiar esas claves temporalesy asignar unas nuevas que permitieran acceder al contenido

Esto es posible cuando el destinatario no está conectado y el mensaje queda almacenado en los servidores de WhatsApp esperando a ser enviado. En ese proceso, el sistema podría generar unas nuevas claves y acceder al contenido del mensaje. Es cierto que este proceso debería hacerse con cada de uno de los mensajes enviados, pero también es cierto que si se repite, se puede llegar a transcribir una conversación completa. ¿Quiere esto decir que nuestros mensajes son accesibles por parte de hackers? No, el cifrado sigue garantizando un estándar de seguridad elevado, pero el problema reside en que WhatsApp podría descifrar el mensaje ante una petición de las autoridades.

¿Qué dice WhatsApp al respecto?

EL PAÍS no ha logrado una respuesta de la compañía, pero un portavoz de la firma ni ha confirmado ni desmentido este extremo a The Guardian, remitiéndose al listado de peticiones de acceso hechas por las autoridades de cada país.

La solución

El usuario puede poner coto de alguna manera a esta posibilidad: para ello es necesario, en la app en el móvil, acceder a Configuración/Cuenta/Seguridad y ahí activar la pestaña “Mostrar notificaciones de seguridad”.

Activando esta opción el usuario será alertado de un posible cambio de claves en la conversación (que puede suceder también cuando el destinatario cambia de móvil). Esta medida no impide que WhatsApp pueda descifrar un mensaje

dado, pero sí alertará al usuario del cambio de claves y podrá optar por dejar de escribir mensajes que podrían ser potencialmente leídos.