Riesgos en el uso de WhatsApp

Madrid, julio 2014 - La aplicación de mensajería multiplataforma WhatsApp se lanzó al mercado en el año 2009 por dos ingenieros de Yahoo. Este sistema utiliza el plan de datos de correo electrónico e Internet del usuario por tanto no tiene un coste adicional. Ha alcanzado los 500 millones de usuarios en todo el mundo (en España su tasa de instalación es superior al 80%, lo que supone que más de 23 millones de personas se han descargado esta aplicación). Sus usuarios comparten más de 50.000 millones de mensajes, 700 millones de fotos y más de 100 millones de vídeos a diario, a lo que hay que sumar, desde agosto de 2013, los mensajes de voz.

El éxito de la aplicación, sin embargo, la ha situado en el punto de mira de los ciberatacantes que, por qué no decirlo, se han encontrado en los diferentes ciclos de vida de la herramienta con una construcción con las puertas abiertas de par en par. Las numerosas vulnerabilidades encontradas la han situado como blanco perfecto para la distribución de malware y robo de datos personales. Esta situación se ha visto agravada por la escasa percepción de riesgos entre los usuarios de dispositivos móviles que apenas si toman precauciones para proteger su información (desde luego muchísimas menos que en otro tipo de dispositivos como los PC).

Las críticas por la pésima gestión de la seguridad se vieron incrementadas en febrero de este año tras anunciarse que Facebook compraba la compañía por 19.000 millones de dólares. En ese momento, se dispararon todas las alarmas con respecto a la pérdida de privacidad y la compartición de datos con la red social líder en el mundo. Incluso el responsable de la oficina de regulación de la privacidad en las comunicaciones en Alemania, Thilo Weichert aconsejó a todos los usuarios de WhatsApp, al día siguiente de la compra, que buscarán alternativas más seguras de mensajería instantánea.

El miedo estriba en la cruce de datos de Facebook con los de los usuarios de WhatsApp en donde se puede acceder a números de teléfono y todos sus contactos, localizaciones GPS, fotografías, vídeos, audios, tarjetas de contacto, gustos, preferencias, etc.

Principales vulnerabilidades

Pero, ¿cuáles son las principales vulnerabilidades en esta aplicación? Desde sus inicios se han ido descubriendo **múltiples fallos de seguridad**, empezando por la falta de cifrado de sus comunicaciones y, por tanto, el acceso a la agenda telefónica y a los mensajes de los usuarios conectados a Internet. Esta situación fue subsanada (eso sí, se ha comprobado que el cifrado es fácil de romper), aunque se ha mantenido otro problema como es el hecho de que la clave de sesión esté basada en el IMEI (Identidad Internacional de Equipo Móvil), un código pregrabado en los teléfonos y que los identifica unívocamente a nivel mundial.

También persisten las **vulnerabilidades en la ubicación del usuario a través del GPS** puesto que WhatsApp almacena las coordenadas geográficas y las mantiene desprotegidas. De este modo, al compartir una ubicación (para lo cual la aplicación necesita la situación en Google Maps) los datos se descargan a través de un canal no seguro, sin utilizar SSL y sin cifrar.

Juan Garrido, consultor de **InnoTec System** (del Grupo Entelgy) descubrió otra gran vulnerabilidad en marzo de 2013. Cualquier usuario, de forma anónima (sin necesidad de credenciales), podía utilizar la infraestructura de WhatsApp para subir todo tipo de archivos o ficheros de cualquier tamaño a sus servidores (incluido los ejecutables). Dado que, además, la plataforma de WhatsApp no cuenta con ningún tipo de antivirus y que los contenidos se borran automáticamente en un período de 30 días, las **facilidades para distribuir todo tipo de malware o realizar ataques de *phishing*** (haciendo creer al usuario que está ante la página web de su banco captando su contraseña) son tremendamente sencillas y sin ningún tipo de costes para el atacante (que además puede mantener el anonimato sin problema)

Asimismo, Garrido descubrió una grave carencia en el proceso de alta y verificación de los usuarios. Así, el código de activación de usuario se genera en el propio entorno de la aplicación, incluso antes de ser enviado a los servidores internos para que éstos manden el mensaje SMS, con el código, al usuario.

El almacenamiento del contenido en sus servidores, la obtención de datos del perfil de usuario, sin necesidad de usar el teléfono móvil, **la ausencia de autorización para enviar mensajes** (con las posibilidades de spam que esto representa), la posibilidad de cambiar el remitente a la hora de enviarlos o el **acceso a las conversaciones** de un usuario a través de otras aplicaciones que tienen acceso a la tarjeta MicroSD (donde se almacenan las copias de seguridad de WhatsApp) son otros de los fallos observados en los últimos meses.

Condiciones de uso y privacidad

Junto con las vulnerabilidades mencionadas, hay otras cuestiones muy relevantes, que van asociadas a las condiciones de uso de la propia aplicación y que no siempre son tenidas en cuenta por sus usuarios. Entre ellas se encuentran las siguientes:

- **La compañía pueda acceder periódicamente a la lista de contactos** y/o libreta de direcciones para mantener un registro de los números de teléfono de otros usuarios (es decir, no existe un consentimiento por parte de los contactos).

- Los datos denominados "Status Submission" (estados, fotos de perfil, información sobre si se está conectado o información sobre la última conexión) tienen una licencia no exclusiva, gratuita y transferible para usarlas, reproducirlas, distribuirlas, crear obras derivadas a partir de ellas, exhibirlas o comunicarlas. De este modo, **todas las actualizaciones de estado son visibles por cualquier usuario de WhatsApp** que tenga el número de teléfono de la persona, sin necesidad de que se haya aceptado previamente. Esta política se hace extensible a los grupos, por lo que si alguien te incluye en un grupo junto con otras personas, cualquiera de los componentes de este grupo tendrá acceso a todos tus datos.

- **Sólo puede ser usado por mayores de 16 años** (o menores con autorización paterna específica)

- **Las condiciones pueden modificarse en cualquier momento, sin avisar**. Es el usuario el responsable de revisarlas periódicamente.

- **No garantiza la confidencialidad** de conversaciones, ni de contenidos intercambiados.

- **Los "Status Submission" no son borrados**, se mantienen en las bases de datos de la compañía

- **Está prohibido el uso comercial de la aplicación** y la utilización de bots que envíen mensajes masivos.

Así pues, y dado que cualquier fotografía, dato o estado del WhatsApp puede ser visto por cualquier persona que, directa o indirectamente, tenga nuestro teléfono, ¿de verdad queremos mostrar a todo el mundo las fotografías de nuestros hijos, nuestro último posado en bañador o nuestros sentimientos más profundos?