Siete riesgos que corres al usar WhatsApp

Desde sus inicios se han ido descubriendo múltiples fallos de seguridad en WhatsApp, la aplicación de mensajería más popular del mundo. El consultor de InnoTec System (del Grupo Entelgy) Juan Garridodescrubrió algunas y te las presentamos a continuación:

1)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, pero se ha comprobado que el cifrado es fácil de romper.

2) 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.

3) 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).

4) 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.

5) 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.

6) La posibilidad de cambiar el remitente a la hora de enviar mensajes 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.

7) 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.

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.

Sólo puede ser usado por mayores de 16 años (o menores con autorización paterna específica), aunque evidentemente es algo que se puede evitar con facilidad.

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.