

"No solucionables", según Facebook

Nuevos problemas de privacidad en Facebook



Recientes vulnerabilidades o errores en la popular red social Facebook tienen como común denominador que Facebook considera que son funcionalidades importantes dentro de su entorno y por lo tanto no pueden eliminarse; es decir, solucionarse.

Diario Ti: Inicialmente, el 18 de julio pasado un investigador español descubrió una vulnerabilidad que permite realizar una redirección abierta [1] desde la plataforma móvil de la red social (m.facebook.com). Esto es que, llevando a cabo un procedimiento sencillo, es posible engañar al usuario para que piense que está ingresando a Facebook cuando en realidad puede estar ingresando a otro sitio. Los delincuentes podrían utilizar este método para cometer fraudes y estafas en Internet.

Facebook admitió este comportamiento anómalo [2] pero dijo "que radica en una funcionalidad que necesitan y, por tanto, prefieren correr el riesgo".

Como consecuencia de este descubrimiento, otro investigador chileno publicó [3] la forma en que es posible obtener en forma automatizada (realizando miles de consultas en forma simultánea y sin control)

si un usuario se encuentra registrado en la red social, simplemente conociendo su correo electrónico o número telefónico. Nuevamente la empresa expresó que "esta habilidad para localizar amigos a través del correo es parte del núcleo de Facebook y si bien puede ser una vulnerabilidad en un sitio financiero, aquí corresponde a una funcionalidad de la red".

Paradójicamente, en forma coincidente con estos hallazgos, Facebook lanzó el programa "Bug Bounty" [4] cuyo objetivo es pagar 500 dólares a quienes descubran vulnerabilidades críticas en la plataforma, similar a lo que hace Google desde 2010. Sobra decir que ninguno de los dos descubrimientos anteriores fue recompensado, porque ni siquiera han sido reconocidos como fallos.

También a finales de julio, en países de habla hispana comenzó a circular un mensaje que informaba que la aplicación de Facebook para todos los smartphones comparte (aún lo hace) la agenda personal del usuario, por defecto y sin informarlo:

"Atención, por motivos que se desconocen, todos los smartphones comparten la información de la agenda personal de uno con la empresa Facebook Inc, compruébenlo ustedes mismos".

Efectivamente, al instalar la aplicación, Facebook automáticamente almacena (no comparte, como se ha informado en forma incorrecta) la información de contacto, fotografías del perfil y calendario con el objetivo de conectar a sus usuarios en algún momento. Al respecto Facebook en su sitio web informa:



"Al activar esta característica se enviarán periódicamente copias de tus contactos del dispositivo BlackBerry a Facebook Inc. para vincularlos y conectarlos con tus amigos de Facebook. Las fotografías de perfil e información sobre ti y tus amigos de la red social también se enviarán periódicamente desde tu Facebook a tu lista de contactos y calendario de BlackBerry. Aceptas que el acceso a estos datos (p.ej. mediante aplicaciones) dejará de estar sujeto a tu configuración de privacidad y la de tus amigos de Facebook una vez que se almacenen en tu dispositivo BlackBerry".

Facebook, a través de su página de fans, ha negado los "rumores" de que esa información sea compartida públicamente y ha dicho que "la posibilidad de ver la agenda ha existido durante mucho tiempo y ha sido diseñada para mostrar una única lista de contactos en vez de tener que visitar cada perfil".

"Rumors claiming that your phone contacts are visible to everyone on Facebook are false. Our Contacts list, formerly called Phonebook, has existed for a long time. The phone numbers listed there were either added by your friends themselves and made visible to you, or you have previously synced your phone contacts with Facebook. Just like on your phone, only you can see these numbers."

Esta afirmación es cierta, ya que la información no es compartida abiertamente para todo el mundo, pero "desde hace tiempo" ha sido tomada del teléfono y almacenada en la plataforma de Facebook, sin informar adecuadamente al usuario.

La información ya compartida puede eliminarse y esta "funcionalidad" puede deshabilitarse [5], pero quien no preste atención a este hecho, al instalar la aplicación estará compartiendo abiertamente toda la información y, lo que es aún peor, también estará brindando esta información a la red social, sin el correspondiente permiso de sus dueños. Para corregir esto se debe ingresar a la red social a través del Smartphone y allí hay una opción que debe deshabilitarse. La dirección de acceso es: www.facebook.com

Finalmente, el motivo de considerar como vulnerabilidad a una supuesta funcionalidad radica en el punto desde donde se observe dicho comportamiento anómalo:

Facebook lo ve desde las ventajas adicionales que el usuario adquiere al utilizar dicha funcionalidad o bien desde los beneficios que obtiene la red social, sin olvidar sus motivos económicos y que su creador ha declarado que "no cree en la privacidad ni en la intimidad".

Las personas que desarrollamos nuestra actividad en seguridad lo vemos desde el punto de vista de la privacidad del usuario y cómo ella es avasallada, simplemente para obtener una ventaja discutible y que, de todos modos, se podría generar de otra manera más confiable.

Independientemente si los hallazgos mencionados deben ser considerados funcionalidades o vulnerabilidades, lo más importante a destacar es que, según la empresa, estos comportamientos, y seguramente muchos otros, obedecen al crecimiento de la red social, lo cual evidentemente está por encima de la privacidad del usuario, que es quien en última instancia termina pagando su acceso, creyendo que es gratis.

[1] Redirección abierta en Facebook por Vicente Aguilera Díaz
seclists.org

[2] Un investigador español detecta una seria vulnerabilidad en Facebook
www.elpais.com

[3] Búsqueda automatizada de cuentas Facebook por Fernando Lagos
blog.segu-info.com.ar
blog.zerial.org

[4] Bug Bounty
www.facebook.com

[5] Configuración de privacidad de la agenda de contactos en Facebook
www.facebook.com
www.facebook.com

Autor: Cristian Borghello - External Security Consultant for ZMA
Fotografía: Cristian Borghello