¿Qué riesgo tienen las 'apps' para móviles en el entorno corporativo?

Revisar qué permisos solicitan las aplicaciones de los móviles cuando se instalan y evitar compartir contraseñas o información sensible a través de estas *apps*. Estas son algunas de las recomendaciones que investigadores del centro tecnológico Barcelona Digital apuntan en un informe sobre los riesgos de aplicaciones como Twitter, Facebook o Whatsapp en teléfonos inteligentes corporativos.

BDigital 18/12/2013 09:00 CEST

Los *smartphones* se han convertido en la principal puerta de acceso al mundo digital. / Cheon Fong Liew

Los *smartphones* se han convertido en la principal puerta de acceso al mundo digital. Gracias a las *apps* se puede acceder desde nuestro teléfono móvil inteligente a un gran número de servicios, muchos de ellos gratuitos y muy populares por su originalidad y utilidad.

Sin embargo, según el informe *Los riesgos de las apps en el entorno corporativo*, realizado por expertos del área de I+D+i Seguridad de Barcelona

Digital, la realidad muestra que la utilización de una aplicación en los dispositivos móviles puede constituir un elemento de riesgo capaz de comprometer la seguridad de la información que genera y almacena.

Este análisis, disponible por web ha identificado estos riesgos y sus causas, mostrando ejemplos de algunas de las apps más populares como Twitter, Facebook o Whatsapp, así como de la forma de prevenirlos y mitigarlos a través de unas sencillas recomendaciones.

Los principales riesgos son la apropiación indebida de la información, el 'secuestro' del dispositivo y la ilegalidad

Según el informe, es común que algunas apps comercialicen información de un usuario obtenida de forma inadvertida a partir del dispositivo móvil donde se ha descargado. Esta información posee un gran valor, puesto que pone de manifiesto hábitos, gustos y preferencias que definen el perfil social del usuario.

Cuando esta apropiación indebida de información se realiza a través de un móvil corporativo se entra en la esfera profesional incluyendo contactos, mensajes, correos electrónicos, relaciones profesionales, proyectos, pensamientos, etc. que pueden comprometer la competitividad de la empresa propietaria del dispositivo.

Entre los principales riesgos asociados a la descarga y uso de *apps* en dispositivos móviles corporativos, se han identificado la apropiación indebida de la información, el abuso o 'secuestro' del dispositivo y el incumplimiento legal y normativo.

Según datos recientes, únicamente el 61% de las 150 aplicaciones más descargadas tienen una política de privacidad clara donde se específica para qué y en qué condiciones va a ser utilizada nuestra información. Además, las aplicaciones que tienen una política de privacidad establecida presentan habitualmente contratos de licencia muy extensos que raramente nadie lee en su totalidad pero que generalmente se aceptan.

Estos contratos están normalmente redactados para definir un entorno de actuación que beneficia claramente a los objetivos y fines de quien explota la aplicación, en detrimento de los derechos de privacidad del usuario. El usuario de las *apps* normalmente tiene una falsa sensación de protección frente a temas de seguridad y privacidad, pensando a menudo que estas condiciones de uso siguen los principios y recomendaciones de la legislación vigente y aplicable en estas cuestiones.

La Patriot Act de EE UU

Sin embargo, al amparo de una legislación diferente, concretamente la Patriot Act en EE UU y unas condiciones de uso aceptadas explícitamente por el usuario, se podría permitir a los propietarios de las appsalmacenar una gran cantidad de información sobre cada uno de nosotros.

Otro riesgo inherente a las aplicaciones es el abuso del dispositivo sin que el usuario sea consciente de ello, como por ejemplo en caso de espionaje o de secuestro del terminal: algunas appspueden ser creadas con motivaciones fraudulentas, y atacar directamente a nuestro terminal para apoderarse de él.

Una vez queda bajo el control del atacante, el dispositivo puede verse involucrado sin el conocimiento del usuario en actividades delictivas, como el robo de información o ataque a otros sistemas informáticos.

Como ejemplos de algunas preocupaciones vinculadas a las *apps* más populares el informe señala el acceso a toda la lista de contactos –que se copia en un servidor externo– (en el caso de Whatsapp), que todos los contenidos subidos a la red social Facebook se convierten de forma automática en propiedad del prestador de servicio, o que el intercambio de mensajes breves con acortadores de url a través de Twitter hace que no tengamos referencia semántica de la web dónde nos dirigimos cuando pulsamos en un enlace de este tipo.

Algunas recomendaciones

Aunque muchos usuarios ya son conscientes de las amenazas de seguridad debido al uso de las ‘apps’, es necesaria una mayor

concienciación sobre los riesgos derivados de la descarga de aplicaciones en dispositivos móviles corporativos. Entre la decena de recomendaciones proporcionadas por los expertos en Seguridad Informática de Barcelona Digital que han realizado el informe, destacan:

- Seguir las reglas de seguridad establecidas por los responsables de Tecnologías de la Información de la empresa, en cuanto a normas de seguridad en el uso del dispositivo móvil corporativo, o bien buscar el asesoramiento especializado de un experto.
- Usar siempre la tienda de aplicaciones oficial del dispositivo.
- Revisar qué permisos solicitan las 'apps' al instalarse y que estos sean apropiados para la función que va a desempeñar.
- Configurar los niveles de privacidad que la aplicación permite.
- Revisar la configuración de geolocalización, y verificar si es necesario o no que esté siempre activada.
- En aplicaciones de redes sociales, no abrir enlaces que provengan de usuarios desconocidos, especialmente cuando estos van en forma de enlaces cortos.
- No compartir contraseñas ni información sensible a través de 'apps'.
- Mantener actualizado el Sistema Operativo.
- Mantenerse informado de las últimas amenazas existentes.
- Tener en cuenta que lo que se comparte por una red social queda permanentemente compartido.

TAGS | SEGURIDAD INFORMÁTICA | SEGURIDAD | APPS | APLICACIONES | MÓVIL | MÓVILES | SMARTPHONES |

La ciencia es noticia