



Amenazas a la Seguridad de los móviles, que deberías tener en cuenta para 2019

La seguridad móvil está en la parte superior de la lista de preocupaciones de todas las empresas en estos días, y por una buena razón: casi todos los trabajadores acceden de manera rutinaria a los datos corporativos desde los teléfonos inteligentes, y eso significa que mantener la información confidencial fuera de las manos equivocadas es un rompecabezas cada vez más complejo.

Si bien es fácil enfocarse en el tema sensacional del malware, la verdad es que las infecciones de malware móvil son increíblemente infrecuentes en el mundo real: la probabilidad de ser infectado es significativamente menor que la de ser alcanzado por un rayo, según una estimación. Esto se debe tanto a la naturaleza del malware móvil como a las protecciones inherentes integradas en los sistemas operativos móviles modernos.

Fuga de datos

La fuga de datos se considera una de las amenazas más preocupantes para la seguridad de la empresa llegando a 2019. ¿Recordás esas probabilidades casi inexistentes de estar infectado con malware? Bueno, cuando se trata de una violación de datos, las empresas tienen una probabilidad de casi **28% de experimentar al menos un incidente en los próximos dos años**, según la última investigación de Ponemon: probabilidades de más de uno de cada cuatro, en otras palabras.

Las fugas que se producen pueden ser resultado de un error manifiesto del usuario, algo tan simple como transferir archivos de la empresa a un servicio de almacenamiento en la nube pública, pegar información confidencial en el lugar equivocado o reenviar un correo electrónico a un usuario no intencionado.

Ingeniería social

La probada y verdadera táctica del engaño es tan preocupante en el frente móvil como en las computadoras de escritorio. A pesar de la facilidad con la que uno podría pensar que se evitarían los engaños de la ingeniería social, siguen siendo sorprendentemente efectivos.

Un **91% de los delitos cibernéticos comienza con el correo electrónico**, según un informe de 2018 de la firma de seguridad FireEye. La firma se refiere a estos incidentes como "ataques sin malware", ya que se basan en tácticas como la suplantación para engañar a las personas para que hagan clic en enlaces peligrosos o proporcionen información confidencial. La empresa dice que **la suplantación de identidad (phishing) creció un 65%** en el transcurso de 2017, y los usuarios de dispositivos móviles corren mayor riesgo de caer en esta situación debido a la forma en que muchos clientes de correo electrónico móvil solo muestran el nombre del remitente, lo que hace que sea especialmente fácil falsificar los mensajes y engañar a una persona para que piense que un correo electrónico es de alguien que conocen o en quien confían.

Interferencia de Wi-Fi

Un dispositivo móvil es tan seguro como la red a través de la cual transmite datos. En una era en la que todos nos conectamos constantemente a redes públicas de Wi-Fi, eso significa que nuestra información a menudo no es tan segura como podríamos suponer.

¿Qué tan importante es esta preocupación? Según una investigación realizada por la empresa de seguridad empresarial Wandera, los dispositivos móviles corporativos usan Wi-Fi casi tres veces más que los datos celulares. Casi una cuarta parte de los dispositivos se han conectado a redes Wi-Fi abiertas y potencialmente inseguras, y **el 4% de los dispositivos se ha encontrado con un ataque de hombre en el medio**, en el cual alguien intercepta maliciosamente la comunicación entre dos partes.

Reflexión

Considerá lo siguiente: en un estudio de Ponemon de 2016, **el 35% de los profesionales indicó que sus dispositivos de trabajo no tenían medidas obligatorias establecidas para asegurar datos corporativos accesibles**. Peor aún, **casi la mitad de los encuestados dijo que no tenía contraseña, PIN o seguridad biométrica para proteger sus dispositivos**, y cerca de **dos tercios dijeron que no usaban cifrado**. El **68% de los encuestados indicó que a veces compartían contraseñas a través de cuentas personales y de trabajo** a las que se accedía a través de sus dispositivos móviles.

El mensaje para llevar a las organizaciones es simple: dejar la responsabilidad en manos de los usuarios no es suficiente.