Relevancia en la industria y herramientas de Seguridad Móvil

Author : M.B.

Date : 25 noviembre, 2018

El trabajo a distancia, es decir el teletrabajo, tiene muchas ventajas, tanto para la empresa como para los empleados. Por ello, las empresas son conscientes de sus beneficios y en algunos países, como Reino Unido, se ha convertido en un derecho de los empleados el solicitar el trabajo móvil [1]. Esto les hace sentir una mayor flexibilidad, libertad y autogestión, lo cual facilita a aquellos que necesitan cuidar de sus hijos o tienen un largo tiempo de desplazamiento para llegar a su lugar de trabajo. Por ejemplo, los empleados remotos no quieren que su gerencia piense que, si no están entregando en los tiempos esperados, es porque el trabajar remotamente los está retrasando. Por lo tanto, trabajarán más que las horas contractuales para alcanzar los objetivos. Además, ayuda a las empresas a reducir costos, especialmente en renta y gastos de consumo (electricidad, agua, servicios de basura, etc.), y encontrar empleados cualificados, independientemente de su ubicación. Con el progreso de la tecnología, la fuerza de trabajo móvil es una tendencia que no va a detenerse. Se prevé que para 2020, el 72,3 por ciento de la mano de obra estadounidense será remota [2].

Los empleados están haciendo negocio desde cualquier dispositivo, haciendo uso de aplicaciones como el correo electrónico o el calendario durante el día e incluso la noche, desde cualquier lugar. Los dispositivos móviles evolucionan convenientemente a una necesidad y pasan a ser de un lujo a un componente necesario, pero crítico para el entorno empresarial. El aumento de las aplicaciones que residen en esos dispositivos conlleva un aumento de retos de seguridad y aseguramiento de los que nunca se había enfrentado la empresa. Es cierto que tanto las organizaciones como los auditores IT se están volviendo más sofisticados en sus enfoques y, por lo tanto, cada vez son más capaces de anticiparse y responder a los retos.

Debido a esto, los expertos profesionales se mantienen de forma constante en una búsqueda de herramientas y técnicas, que pueden aplicar y adaptarse para ayudar a las organizaciones a garantizar que los dispositivos están protegidos adecuadamente. A continuación, os expondré herramientas de 4 categorías que están disponibles de forma gratuita, open source, etc. Debo destacar que las siguientes herramientas pueden ayudar a resolver problemas específicos de seguridad y seguridad en relación con el entorno móvil. [3]

- Herramientas de prueba de aplicaciones móvil

Las herramientas de proxy web, como Burp Suite y ZAP de Open Web Application Security Project (OWASP) son excelentes opciones. Permiten a los usuarios analizar el tráfico entre cualquier dispositivo y las aplicaciones web con las que interactúan. Un proxy de prueba web intercepta los mensajes intercambiados por el dispositivo y la aplicación y permite la manipulación de algunos parámetros, por ejemplo las cabeceras HTTP.

- Herramientas de prueba de dispositivo móvil

Las pruebas especificas de los propios dispositivos móviles incluyen las aplicaciones maliciosas y el comportamiento del usuario ante una situación como phishing. Para ello, se puede hacer uso de la herramienta Dagah de Shevirah.

- Herramientas forenses móvil

La técnica de forense consiste en investigar un dispositivo y determinar si éste ha sido atacado o evaluar de otra manera un incidente potencial que pueda afectarle. La distribución de Santoku Linux se centra en el examen forense de dispositivos móviles. Otras plataformas de pruebas y respuesta a incidentes son Kali y CAINE que contienen herramientas de análisis móviles.

- Herramientas de gestión Sistemas Operativos

Desde el punto de vista de la administración de dispositivos, también hay algunas opciones que se adaptan a cada sistema operativo. Los sistemas operativos iOS y Android tienen incorporados los suyos propios, que les permite realizar tareas como borrado remoto en caso de un dispositivo borrado o perdido.

- Configurador de Apple

- Administrados de dispositivos Android

Existen otras herramientas que proporcionan herramientas de privacidad (The Guardian Project) y configuraciones de sistemas operativos reforzados (CopperheadOS).

Referencias:

[1] GOV.UK, «Flexible working», acceso 15 de noviembre de 2018,https://www.gov.uk/flexible-working .

[2] «Today's mobile workforce: any time, any place», The Telegraph, 5 de septiembre de 2016, acceso 15 de noviembre de 2018, https://www.telegraph.co.uk/business/ready-and-enabled/todays-mobile-workforce-any-time-any-place/

[3] Ed Moyle, «Tools: Mobile Security Tools on a Budget» ISACA Journal, volume 4 (2017): 52 - 53