Publicado en Madrid el 27/09/2017

De la detección al análisis: MobileIron Access amplía el ciclo de vida de la seguridad en la nube

Introduce las funcionalidades Enterprise Risk Discovery y Authentication Analytics, ofreciendo un modelo de seguridad unificado para Mac y PC. Este modelo representa una nueva fase para la seguridad en la nube, en la que intervienen las herramientas que detectan los riesgos, el acceso condicionado basado en el usuario, el dispositivo y la aplicación, las analíticas y la generación de informes, así como la capacidad de hacer llegar esta tecnología a todos los puntos de conexión

MobileIron (NASDAQ: MOBL), la “piedra angular” de la seguridad para las empresas multinube, ha anunciado hoy el lanzamiento de nuevas funcionalidades que refuerzan el ciclo de vida de MobileIron Access, su solución de seguridad en la nube.

MobileIron Access Risk Discovery identifica las apps y dispositivos no autorizados que acceden a servicios empresariales en la nube como Office 365 y Salesforce.

MobileIron Access for Mac and PC ofrece Acceso condicional al PC de sobremesa, garantizando que solo los dispositivos Mac, Windows 10 y Windows 7 de confianza puedan acceder a estos servicios.

MobileIron Access Authentication Analytics identifica patrones de uso poco frecuentes, que puedan ser indicio de un nuevo requisito empresarial o de una potencial amenaza de seguridad.

MobileIron Access ofrece a las organizaciones una arquitectura de seguridad unificada, con el fin de facilitar y proteger los servicios empresariales que prefieran utilizar sus empleados en la nube.

Los servicios no autorizados en la nube se propagan sin control

Preguntando a un director de Sistemas de Información cuántas aplicaciones y servicios en la nube utiliza su empresa, es probable que estime que entre 30 y 40. Pero la realidad demuestra que, por lo general, las empresas tienen más de 900 aplicaciones en su red ampliada, que en su mayoría fueron adoptadas sin aprobación o supervisión informática (*).

Los dispositivos y las aplicaciones en la nube suponen graves riesgos para la seguridad

Existen una serie de riesgos de seguridad entre los dispositivos, las aplicaciones y los servicios a los que se conectan. Estos son algunos ejemplos:

Un dispositivo con modificaciones no autorizadas (jailbroken): un empleado utiliza la app móvil de

Office 365 para acceder a los datos desde un dispositivo con jailbreak. Los datos empresariales estarán entonces accesibles desde dispositivo pirateado

Un PC o un Mac no autorizado: un empleado sincroniza archivos de Google Drive en un dispositivo personal. Los datos empresariales estarán entonces accesibles desde un dispositivo no seguro.

Una app en la nube no autorizada: un comercial descarga una de las docenas de apps que utilizan API para conectarse al servicio en la nube de salesforce.com. Los datos empresariales se encuentran ahora accesibles desde una app móvil no segura.

Para más información: https://www.mobileiron.com/access
(*) Informe Shadow Data de la segunda mitad de 2016 de Cloud Threat Labs & Symantec Cloud SOC (2H 2016 Shadow Data Report).

Acerca de MobileIron
MobileIron proporciona la base segura para que las compañías de todo el mundo se transformen en “Mobile First”. Para más información: www.mobileiron.com.

Datos de contacto:
Amparo Torres Menéndez
AT&A Comunicación Corporativa
669840176

Nota de prensa publicada en: Madrid

Categorías: Software Ciberseguridad Dispositivos móviles