Publicado en Mountain View, California el 07/03/2016

Más del 50% de las empresas tienen dispositivos móviles que no cumplen con las normativas

MobileIron Security Labs publica la primera revisión de riesgos y seguridad para móviles. Según Michael Raggo, director de MobileIron Security Labs: "Las amenazas móviles, tanto internas como externas, están en aumento, y la cadena de seguridad empresarial es tan fuerte como su enlace más débil. El riesgo real es que las empresas subestimen la gravedad del problema. Un único dispositivo dañado que no sea detectado constituye una violación"

PRNewswire/ - MobileIron Inc.(NASDAQ: MOBL), líder en seguridad empresarial móvil, presentó hoy su nueva división de investigación, MobileIron Security Labs (MISL), y la primera publicación de MISL: la Q4 2015 Mobile Security and Risk Review (Revisión de Riesgos y Seguridad para Móviles del Cuarto Trimestre de 2015). El Informe de Riesgos y Seguridad para Móviles del 4º Trimestre de 2015 aborda un conjunto específico de amenazas y riesgos, incluidos los fallos de cumplimiento, dispositivos dañados y riesgos de pérdidas de datos, no cubiertos en otros informes sobre seguridad. El Informe de Riesgos y Seguridad para Móviles finaliza con recomendaciones para fortalecer las implementaciones empresariales móviles.

"Las amenazas móviles, tanto internas como externas, van en aumento, y la cadena de seguridad empresarial es tan fuerte como su enlace más débil", declaró Michael Raggo, director de MobileIron Security Labs. "Un único dispositivo dañado puede introducir malware en la red empresarial o permitir el robo de datos empresariales sensibles que estén alojados detrás del muro cortafuegos".

Más del 50 % de las empresas tienen al menos un dispositivo que no cumple con la normativa
Un dispositivo móvil puede no cumplir con la normativa por una variedad de motivos, como que el usuario deshabilite la protección del número de identificación personal (PIN), pierda un dispositivo, carezca de políticas actualizadas, etcétera. Los dispositivos que no cumplen con la normativa generan un espacio de ataque más amplio para el malware, las usurpaciones y el robo de datos.

"El riesgo real es que las empresas subestimen la gravedad del problema", continuó Raggo. "Un único dispositivo dañado que no sea detectado constituye una violación. No importa si una compañía pierde millones de registros o solo uno; aún así es una violación. Para todas las compañías, pero especialmente para las que operan en sectores altamente regulados, este es un problema enorme".

Los dispositivos dañados han aumentado un 42 %
Se considera que un dispositivo está dañado cuando registra una fuga o una filtración; su incidencia aumentó de manera marcada durante el último trimestre del año, en el que se constató que una de cada 10 empresas tenía al menos un dispositivo dañado. Por otra parte, es interesante tener en cuenta que durante ese trimestre la cantidad de empresas con dispositivos dañados aumentó un 42%. Al mismo tiempo, los atacantes maliciosos utilizan diferentes herramientas para que resulte más difícil identificar los dispositivos dañados. MISL ha encontrado variantes de herramientas de fuga, así como herramientas antidetección que esconden el hecho de que un dispositivo tiene una fuga y, así, crean

un falso sentido de seguridad en caso de que no se detecte.

Otras conclusiones destacadas de la investigación son las siguientes:

Menos del 10% de las empresas ejecutan parches que dejan al dispositivo vulnerable a la pérdida de datos.
El 22% de las empresas tenía usuarios que habían quitado el PIN que elimina la primera línea de defensa.
Más del 95% de las empresas no cuentan con protección ante malware móvil.

Para descargar la Revisión de Riesgos y Seguridad para Móviles, incluida la lista negra de las principales aplicaciones móviles, visite:https://www.mobileiron.com/q4-mobile-security-review.

La Revisión de Riesgos y Seguridad para Móviles del Cuarto Trimestre de 2015 se basa en datos totales y anónimos compartidos por clientes que fueron compilados entre el 1 de octubre de 2015 y el 31 de diciembre de 2015.

MobileIron ofrece una base segura para que las compañías de todo el mundo se conviertan en organizaciones Mobile First. Para obtener más información, visite www.mobileiron.com.
Logo: http://photos.prnewswire.com/prnh/20140923/147891
Descargue el informe: https://info.mobileiron.com/Q42015-MobileSecurityandRiskReview_LandingPage.htmlInscríbase al webinar el martes 15 de marzo a las 10 AM PT: https://www.mobileiron.com/en/resources/webinars/mobileiron-q4-mobile-security-and-risk-review
Contacto: Clarissa Horowitz, MobileIron, clarissa@mobileiron.com, +1-415-608-6825

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

Nota de prensa publicada en: Mountain View, California

Categorías: Software Ciberseguridad Dispositivos móviles