Artículo sobre la SEGURIDAD EN DISPOSITIVOS MÓVILES

Avendaño Avendaño, Ivan.
Iavenda80_4@hotmail.com
Universidad Piloto de Colombia

***Resumen*—Este documento presenta un breve análisis sobre la seguridad en los dispositivos móviles, las amenazas y vulnerabilidades latentes, el estado actual y la creciente propagación de código malicioso, el impacto del uso de estos dispositivos en las organizaciones y por último un acercamiento de cómo alinear el gobierno y la política interna de la organización mediante marcos de referencia para la implementación de controles que permitan el uso de los equipos móviles dentro las compañías.**

***Índice de Términos*— Amenazas, BYOD, Móviles, Seguridad.**

***Abstract*—This paper presents a brief analysis of security in mobile devices, the latent threats and vulnerabilities, the current state and the increasing spread of malicious code, the impact of the use of these devices in organizations and finally an approach of how to align the government and the internal politics of the organization by reference frames for the implementation of controls that allow the use of mobile devices within companies.**

***Key Words*— BYOD, Mobile, Security, Threats**

I. INTRODUCCIÓN

ESTE DOCUMENTO ES UN BREVE ANÁLISIS SOBRE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES. Debido al creciente desarrollo de las comunicaciones y la tecnología en el mundo cada vez nos enfrentamos a nuevos retos en nuestra vida tanto personal como laboral. Las organizaciones tienen que estar siempre a la vanguardia y vivir al ritmo del mundo actual.

Los nuevos dispositivos permiten la facilidad de conectarse con el mundo en cualquier lugar y a cualquier hora, los teléfonos inteligentes y el uso de tablet hacen posible que se mantenga frecuentemente una comunicación con las empresas, familia y amigos; así mismo estos dispositivos cuentan con grandes cantidades de almacenamiento y son rápidos al momento de procesar datos y enviarlos por medio de la red, por tal razón mantener la protección de la información cada día es más complejo y requiere una mayor participación de la alta dirección en las empresas y un compromiso por parte de los usuarios finales en cultura de seguridad y protección de la información.

II. AMENAZAS, VULNERABILIDADES, ESTADO ACTUAL

Como se mencionó en la parte introductoria de este documento, los dispositivos móviles permiten estar conectados en la red las 24 horas del día, mantener y almacenar datos, tienen aplicaciones para realizar transacciones bancarias, mensajería instantánea entre otras; por consiguiente ahora son frente de ataques con un número importante de código malicioso (Malware) en la red dispuesto a atacar los sistemas operativos y/o las transacciones realizadas por este medio. Se hará una revisión de las amenazas, vulnerabilidades y un vistazo general del estado actual de detección según fuentes publicadas por los fabricantes de software de protección.

A. Amenazas

Una de las principales amenazas de los dispositivos móviles sin lugar a duda, es el código malicioso, este se transmite fácilmente y en especial por medio de las redes abiertas, los equipos pueden entrar y salir de redes y así mismos transportar cualquier tipo de malware sin control, igualmente las aplicaciones que son descargadas pueden contener virus u otro tipo de código malicioso que pueda comprometer la información personal del usuario o ser utilizado para que un atacante pueda acceder a una compañía para extraer información o afectar la disponibilidad de los servicios de la misma. Los dispositivos móviles son blanco fácil de hackers, muy pocos usuarios colocan claves de seguridad a los equipos o si existen estas carecen de complejidad haciendo fácil su descubrimiento. Hurtos o pérdida de los dispositivos, el mercado negro de equipos móviles hace que se incremente el

robo de estos dispositivos, según una publicación realizada en el mes de febrero por el diario universal, en Bogotá se roban cada dos minutos un equipo móvil, lo que implica perdida de información valiosa almacenada en la tarjeta SIM o en las memoras flash de los dispositivos, sin contar con otro tipo de información como correo electrónico, agendas personales, sitios con claves de acceso configuradas, entre otros.

B. Vulnerabilidades y Controles

Se describieron algunas de las amenazas importantes y relevantes que están latentes en la red, pero si sumado a esto los equipos son vulnerables y no crean contramedidas para mitigar el riesgo esto hará que sean más fáciles de ser explotados por un atacante. La principal vulnerabilidad así como la amenaza asociada radica en la falta de protección (antivirus) en los dispositivos móviles, permitiendo la fácil propagación de malware, particularmente cuando se accede a redes públicas sin ningún tipo control de seguridad, hay una alta exposición de permitir que atacantes accedan a nuestros dispositivos móviles para el robo de información o para colocar troyanos, gusanos o cualquier otro tipo de virus, que posteriormente pueda ser usado para ataques en las redes de las organizaciones, por eso es importante mantener actualizados los dispositivos y contar con software de protección de fabricantes reconocidos con relación a la instalación de este tipo de productos, los usuarios se pueden remitir a estadísticas o herramientas como por ejemplo el cuadrante de Gartner http://www.gartner.com/technology/reprints.do?id=1-1PCNX43&ct=140109&st=sb. Los dispositivos no se encuentran cifrados, el no colocar ningún tipo de protección de los datos almacenados en el equipo, hace que sean más vulnerables al robo de información, por esa razón se debe activar el mecanismo de cifrado nativo que traen o buscar alternativas como las ofrecidas por algunos fabricantes como Microsoft http://technet.microsoft.com/es-es/library/cc162802.aspx. No usar claves o que estas no sean seguras, esta práctica ha mejorado en los usuarios, sin embargo las contraseñas siguen siendo débiles por lo tanto se debe mantener una clave segura que no sea fácil de romper. Comunicación vía Bluetooth, en ocasiones se puede dejar sin ningún tipo de protección a un equipo luego de realizar una conexión, se recomienda mantener siembre inactiva esta opción y solo activarla en el momento de ser usada así mismo el uso de claves de acceso para la comunicación segura es muy importante. Cuidado de los dispositivos, si bien es cierto que los equipos móviles se hicieron para ser usados en lugares públicos, se debe mantener una cierta cautela al momento de usarlos en especial en aquellos lugares de alta exposición, según artículo publicado por el diario el tiempo, en Bogotá se concentra el robo de celulares en 5 localidades, en estas zonas se presentaron 2.599 casos, lo que representa el 45 por ciento del total de los reportes http://www.eltiempo.com/archivo/documento/CMS-13338095.

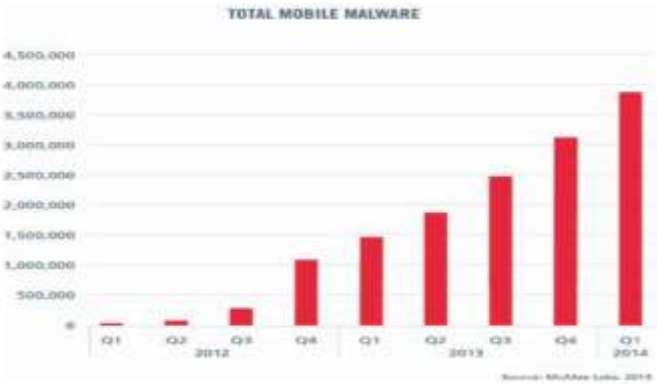

Fig. 1. Tendencia de malware en equipos móviles
Fuente: McAfee Threats Report June 2014

C. Estado Actual

Según cifras de algunos fabricantes la propagación de código malicioso y de ataques dirigidos a equipos móviles es cada vez más alta. El último reporte entregado por McAfee y publicado en el mes de junio de 2014, indica que en tan solo un año el número total de muestras de malware móvil ha crecido en un 167%. La siguiente gráfica muestra el incremento en los últimos años de código malicioso detectado para Smartphone.

Orto dato importante es la cobertura de ataque, según McAfee, la superficie de ataque se incrementa en dispositivos con aplicaciones, ya que estas requieren en muchas oportunidades la entrega

de permisos especiales permitiendo que atacantes puedan acceder a archivos de las tarjetas SD o información de cuentas de correo registradas en las aplicaciones, entre otros.

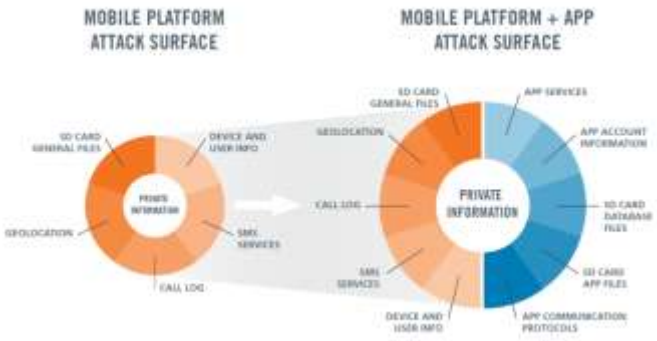

Fig. 2. Superficie de ataque en dispositivos móviles
Fuente: McAfee Threats Report June 2014

ESET publicó en el 2012 un reporte en donde tipifica los sistemas operativos con mayor cobertura en el mercado y que por ende presenta el mayor número de ataques, esta lista la encabeza Android con el 43%, así mismo F-Secure público en su reporte del segundo Q del 2014 que en los dispositivos con sistemas operativos Android, se han encontrado 275 nuevas amenazas o variantes, y tan solo 1 para iPhone. http://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf

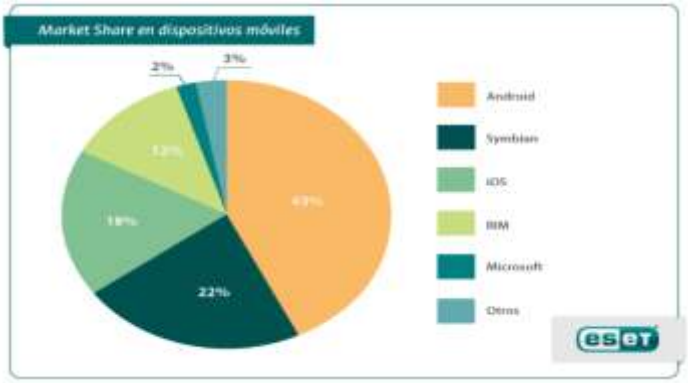

Fig. 3. Participación en el mercado de sistemas operativos
Fuente: ESET Malware en Dispositivos Móviles

Para aquellas personas que quieran endurecer sus dispositivos algunas páginas en internet nos ofrecen concejos de cómo mantener los equipos protegidos. http://androidayuda.com/2014/04/29/android-es-lider-mundial-en-malware-como-protegernos/.

Por otro lado, y no menos importante es conocer desde donde se presentan ataques (Ver Fig.3), Japón, y Estados Unidos encabezan la lista, los países latinoamericanos presentes son Brasil y Chile esto nos sirve para tener una referencia geográfica de donde se concentran o incrementan los riesgos hacia los teléfonos inteligentes y en general a cualquier dispositivo tecnológico.

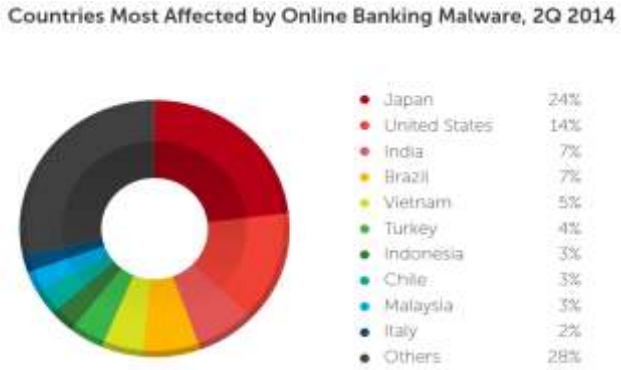

Fig. 3. Tendencia de ataques informáticos por país
Fuente: Trend Micro Turning the Tables on Cyber Attacks Responding to Evolving Tactics

III. IMPACTO EN LAS ORGANIZACIONES, USO DE BYOD

Como se mencionó anteriormente en las dos anteriores secciones, vemos como los dispositivos inteligentes cada vez son más foco de ataques, la preocupación ahora es para las organizaciones, si pensamos que la gran mayoría de usuarios de Smartphone utilizan sus unidades de almacenamiento para llevar y traer información de las compañías, o son utilizados para realizar consultas de correo electrónico y a esto se suma el creciente número de código malicioso y vulnerabilidades detectadas en los sistemas operativos, el riesgo es más alto y mantener la confidencialidad, integridad y disponibilidad de la información en la compañía es mas critica. Por lo tanto, el reto para los grupos de seguridad en las organizaciones es crear políticas y contramedidas que ayuden con la protección de la información, pero lo más importante es crear la cultura de seguridad en los usuarios finales y hacer entender la importancia de mantener protegida la información. Con la tendencia de algunas organizaciones de implementar la política de trae tu propio dispositivo (BYOD), se recalca la necesidad de mejorar las políticas de seguridad de las organizaciones y la cultura de los usuarios, IBM resalta la importancia de tener y mantener una administración

centralizada, así mismo propone alternativas para controlar las aplicaciones que son instaladas en los dispositivos móviles de los empleados. El Mobile Device Management (MDM), es un tipo de software que permite asegurar, monitorear y administrar dispositivos móviles, realizar instalación masiva de aplicaciones, seleccionar aplicaciones, rastreo satelital, sincronización de archivos, bloqueo de funciones, control de gastos, borrado remoto, aplicar contraseñas, entre otras; ¿pero estas medidas se puede implementar sin afectar la privacidad de la información o vulnerar los derechos de los empleados?, es el interrogante que surge, leyes como la 2774 del 16 de agosto del 2013 en donde se restringe el uso de bloqueadores de señal o las de protección de datos personales como la 1581 del 2012 pueden hacer que medidas como estas no sean respaldadas jurídicamente y las organizaciones entren en una encrucijada legal, no se abordara en el detalle de este tema, pero debe ser tenido en cuenta al momento de diseñar e implementar políticas y controles de seguridad para dispositivos móviles en las compañías.

IV. MARCOS DE REFERENCIA Y LINEAMIENTOS DE GOBIERNO ORGANIZACIONAL EN LA POLÍTICA INTERNA

ISACA después de liberar la versión 5 de COBIT, ha publicado una serie de documentos los cuales servirán para apoyar a las aéreas de IT, seguridad de la información y gobierno corporativo con la implementación de controles y buenas prácticas de administración, uno de los documentos y que ha servido de material de apoyo para este artículo es Seguridad en dispositivos móviles usando Cobit 5.

El propósito principal de esta publicación es establecer un marco de gestión uniforme y dar orientación sobre la planificación, ejecución y el mantenimiento integral de seguridad para dispositivos móviles en el contexto de empresas, así como la gestión apropiada de riesgos utilizando COBIT 5 como el marco general de referencia. Vemos como se plantean algunos controles que pueden ser implementados (Ver fig. 4), entre los que se destacan: extender las medidas de protección (antivirus) a dispositivos móviles, utilizar mecanismos o herramientas para identificación y autenticación de dispositivos, extender las políticas de hardening o de inicio de sesión único al equipo móvil.

COBIT 5 Process	Summary Description	Application to Mobile Device Security
DSS05.01 Protect against malware.	Implement measures to protect enterprise IT from the various types of malware.	Extend protective measures (e.g., third-party tools) to mobile devices, and ensure that they are functional and effective autonomously, without users having to bring in the device.
DSS05.02 Manage network and connectivity security.	Implement measures and restrictions for authentication, authorization and data transmission.	Use preapplied (device) controls to protect connectivity. Use additional tools for encryption and network/ device identification and authentication.
DSS05.03 Manage endpoint security.	Implement a security level equivalent to or greater than the normal organizational security level.	Use preapplied (device) controls to harden the device. Implement remote command and control to maintain system integrity.
DSS05.04 Manage user identity and logical access.	Manage rights in accordance with business needs and degree of risk/exposure.	Use preapplied (device) controls to enforce multifactor access. Extend existing practices, e.g., single sign-on, to the mobile device as appropriate.

Fig. 4. Controles Cobit
Fuente: ISACA Securing Mobile Devices Using COBIT® 5

Otro documento publicado por ISCA y que puede ser muy útil para las aéreas de cumplimiento es Bring Your Own Device (BYOD) Security Audit/Assurance Program, es una herramienta para ser usado como guía en los procesos de auditoría por los profesionales encargados de la validación y el cumplimiento de los controles de TI.

En cuanto a la norma ISO 27001:2013 incluye en el dominio de organización de la seguridad de la información, un control enfocado a la creación de políticas de seguridad que permitan la gestión de los riesgos asociados a la introducción de dispositivos móviles en las compañías.

NIST cuenta con la publicación SP 800-124 Rev. 1, el propósito de esta publicación es ayudar a las organizaciones a gestionar de forma centralizada la seguridad de los dispositivos móviles, esta guía ofrece recomendaciones para la selección, implementación y uso de tecnologías de gestión centralizada, y explica los problemas de seguridad inherentes en el uso de dispositivos móviles así mismo ofrece recomendaciones para proteger los dispositivos móviles a través de sus ciclos de vida. Así mismo NIST realizó una publicación especial para el análisis forense de dispositivos móviles, el documento SP 800-101 (Draff) es una guía que trata de profundizar en los dispositivos móviles y explicar las tecnologías involucradas y su relación

con los procedimientos forenses, también contiene procedimientos para la convalidación, conservación, adquisición, exploración, análisis y reporte de la información digital.

Luego de mencionar los marcos de referencia COBIT, ISO27001 y NIST; vemos que las organizaciones cuentan con los instrumentos necesarios para modificar sus políticas actuales y estas se encuentren alienadas de acuerdo con las necesidades cambiantes del mundo y la tecnología, recalcando la necesidad que en la administración del riesgo sean incluidos los dispositivos móviles de los usuarios como parte de los activos de la organización y del tratamiento de riesgo según los resultados de la valoración obtenidos.

V. Conclusiones

Es importante mantener una correcta protección de nuestros dispositivos como: claves de seguridad robustas, software de protección, cifrado de datos, políticas de seguridad en nuestras organizaciones, pero ante todo debemos tener una cultura de seguridad y conciencia sobre la importancia del cuidado de la información y la protección de datos. "Las Personas, el eslabón más débil de la Seguridad de la información".

REFERENCIAS

[1] *ISACA Securing Mobile Devices Using COBIT® 5 for Information Security*, USA, 2013.

[2] *ISACA Bring Your Own Device (BYOD) Security Audit/Assurance Program*, USA, 2013

[3] *Incontec Norma Técnica NTC-ISO-IEC Colombiana 27001*, ISO/IEC 27001: 2013.

[4] *NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication 800-124 Revision 1, 2013

[5] *NIST Guidelines on Mobile Device Forensics (Draft)*, NIST Special Publication 800-101 Revision 1, 2013

[6] *McAfee Threats Report*, McAFEE LABS, June 2014

[7] *ESET Malware en Dispositivos Móviles*, ESET Latinoamérica, 2012

[8] *F-Secure Mobile Threat Report*, F-Secure Labs, 2014

[9] *Trend Micro Turning the Tables on Cyber Attacks Responding to Evolving Tactics*, Trend Micro Labs, 2014

[10] J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com

[11] Semana. (2014, Enero 30). Title. Tome precauciones si se conecta a una red pública [Online] Available: http://www.semana.com/tecnologia/tips/articulo/tome-precauciones-conecta-red-publica/373143-3

[12] Androidayuda. (2014, Abril 29). Title. Android es líder mundial en malware, ¿cómo protegernos? [Online] Available: http://androidayuda.com/2014/04/29/android-es-lider-mundial-en-malware-como-protegernos/

[13] F-Secure. (2014). Title. Threat Report H12014 [Online] Available: http://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf

[14] Microsoft. (2007, Mayo 29). Title. Kit de herramientas de cifrado de datos para equipos móviles: guía de implementación y planeación [Online] Available: http://technet.microsoft.com/es-es/library/cc162802.aspx.

[15] Wikipedia. (2014, Mayo 29). Title. Mobile device management [Online] Available: http://es.wikipedia.org/wiki/Mobile_device_management

[16] Eltiempo. (2013, Agosto 21). Title. Gobierno restringe el uso de bloqueadores de señal de celular [Online] Available: http://www.eltiempo.com/archivo/documento/CMS-13006719

[17] Eluniversal. (2014, Febrero 9). Title. Cada dos minutos se roban un celular [Online] Available: http://www.eluniversal.com.co/colombia/cada-dos-minutos-se-roban-un-celular-151089

Autor

Ing. Ivan Avendaño Avendaño.
Líder de Calidad y Mejoramiento Continúo
Líder Auditor en Seguridad y Riesgos Informáticos
Auditor Interno ISO20000
ITIL® Foundation Certificate in IT Service Management