LOS DISPOSITIVOS MÓVILES Y LA FUGA DE INFORMACIÓN

Bravo Bermejo, Jose Parmenio.
Josebravo_7010@hotmail.com
Universidad Piloto de Colombia

Resumen - en este análisis podemos observar las amenazas de los dispositivos móviles en nuestras empresas al permitir el acceso a los datos corporativos, convirtiéndose en un riesgo eventual para la fuga de información de la Entidad.

Términos: Dispositivo móvil, fuga de información, política de seguridad, software malicioso.

Abstract - In this analysis we can see the threats of mobile devices in our companies to allow access to corporate data, becoming a potential risk for information leakage Entity.

Terms: Mobile device, information leakage, security policy, malicious software.

I. INTRODUCCIÓN

La falta de seguridad de la información hace parte del día a día de las organizaciones, donde es necesario tomar conciencia y generar medidas de prevención con el fin de mitigar el riesgo de fuga de información.

La tecnología desempeña un papel bastante importante en nuestras vidas, las operaciones diariamente las vemos plasmadas en nuestros equipos de cómputo, celulares, tabletas y cualquier instrumento que nos permite conectarnos a una red, con el mayor uso de información también aumenta el volumen y formas de las amenazas, los cibercriminales buscan diariamente explotar nuevas vulnerabilidades para el acceso a los datos corporativos con el fin de robar la información.

Frente a este evento es preciso que las empresas u organizaciones diseñen un sistema de gestión para prevenir la fuga de información mediante los dispositivos móviles, este diseño reduce el riesgo de fuga de información y protege los datos esenciales de las Entidades.

II. PROCEDIMIENTO DE ANÁLISIS

A. Amenazas de los Dispositivos Móviles

Con el aumento del número de personas que utilizan dispositivos móviles para navegar por la web, se han acrecentado los riesgos de seguridad para las empresas, donde los cibercriminales y el malware centran cada vez más los ataques en los instrumentos portables, para el robo de datos corporativos y/o personales.

Las empresas especializadas en productos para la seguridad informática han podido identificar diferentes ataques desde los dispositivos móviles que sobresalen en Latinoamérica.

La mejor defensa contra las amenazas de los dispositivos móviles y los códigos maliciosos, es estar actualizados con parches de aplicaciones de antivirus y usar contraseñas difíciles de descifrar para el servidor e implementar una estrategia de seguridad.

Asegurarse de que su política de seguridad cubre adecuadamente a los dispositivos móviles, incluyendo:

- Gestión de amenazas – identificación y eliminación de virus, programas espía y spam.

- Control de acceso y administración – política de contraseñas y administración de aplicaciones.

- Protección de datos – encriptado de datos confidenciales en dispositivos y eliminación remota de datos.

- Control de acceso a redes – política de acceso mediante conexiones VPN a través

de redes públicas, validación de dispositivos al conectarse a la red de la empresa.[1]

B. Software malicioso para dispositivos móviles

Los primeros ejemplos de este tipo de programas maliciosos aparecieron en 2004. Estaban dirigidos al sistema operativo Symbian, pero dieron lugar a muchas otras amenazas para dispositivos móviles.

Desde aquel momento, los cibercriminales han desarrollado software malicioso para la nueva generación de teléfonos inteligentes con sistemas operativos Android e iOS, desde entonces se han descubierto miles de programas maliciosos para dispositivos móviles.

Los cibercriminales también aprovechan las vulnerabilidades en los dispositivos móviles los cuales se derivan de errores de programación que bajo determinadas circunstancias pueden comprometer un sistema y robar información.

Pese a esto, en la actualidad se observan más casos de explotación de vulnerabilidades que afectan a sistemas "tradicionales" y no plataformas Mobile, sin embargo, en 2013 ha quedado de manifiesto que los cibercriminales están comenzando a enfocarse cada vez más en explotar agujeros de seguridad en sistemas operativos para móviles como Android.

Así mismo, una encuesta mundial a usuarios de móviles indicó que 38% de los usuarios de teléfonos celulares había experimentado delitos cibernéticos móviles en alguna de sus modalidades. Los dispositivos perdidos o robados suelen precipitar actividades móviles maliciosas, aunque el comportamiento imprudente de los usuarios de teléfonos celulares los vuelve susceptibles a muchos tipos de ataques.

Los usuarios de los dispositivos móviles manifiestan que tienen una conducta imprudente cuando almacenan archivos sensibles en el teléfono, guardan información laboral y personal en las mismas cuentas de almacenamiento en línea y comparten las claves de acceso con familiares y amigos, lo cual pone en riesgo sus datos y algunas veces los de sus empleadores. [2]

C. Fuga de información y amenazas cibernéticas

El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil.

Las organizaciones contienen una cantidad de información confidencial y de propiedad intelectual, y cada vez más empresas, podrían ser víctimas de fugas de datos de alto perfil. La mayoría de las fugas de datos son accidentales o involuntarias, pero toda fuga tiene el potencial de ser devastadora y las pérdidas pueden ser importantes. Es posible evitar las fugas de datos y mantener a las organizaciones seguras sin inhibir las operaciones.

En términos generales, durante 2014 y el primer semestre de 2015, la Policía Nacional ha atendido 14.222 casos relacionados con amenazas cibernéticas, que van desde el robo de identidad, hasta los hurtos electrónicos, accesos abusivos a sistemas informáticos y pérdida de información sensible en las organizaciones.

En los últimos años, se han detectado múltiples intentos de ataque a la infraestructura crítica del país; estos intentos han sido neutralizados exitosamente hasta el día de hoy, sin embargo, su nivel de sofisticación cada vez es mayor y por lo tanto se requiere un equipamiento de última tecnología y una excelente preparación del personal a cargo de la seguridad nacional de Colombia. [3]

D. 10 Años de Fuga de Información

Estos ataques se presentan a nivel mundial, el último incidente importante fue el relacionado con Sony Pictures Entertainment a finales de

noviembre del 2014. Es importante hacer un recuento de las mayores fugas de información en los últimos diez años.

A partir de una recopilación pública de datos publicados en DataBreaches y por el Indentify Theft Resource Center de las brechas de seguridad que se han hecho públicas en los últimos 10 años y en las cuales se han filtrado por lo menos **30.000 registro**s, vale la pena anotar que en la lista de empresas afectadas por estas brechas de seguridad encontramos a Gmail, eBay, Adobe, Sony, Target y AOL entre otras grandes empresas que llegan a manejar grandes volúmenes de información sensible; esto no quiere decir que las empresas más pequeñas no sean vulnerables a este tipo de incidentes.

Las empresas que más buscan afectar los atacantes se encuentra en una de las siguientes categorías:

- Empresas web
- Financieras
- Empresas de salud
- Gobiernos
- Compañías de retail

El restante son empresas de transporte, energía, académicas y telecomunicaciones, entre algunas otras.

La mitad de los incidentes están relacionados con ataques externos y una cuarta parte tiene que ver con equipos o dispositivos perdidos o robados con información sensible, el restante está entre información publicada accidentalmente, casos de fraude interno y niveles pobres de seguridad. [4]

E. Como mitigar la fuga de información

Hoy en día es indispensable para una empresa proteger y controlar la información confidencial, siendo todo un reto ya que deben considerarse las amenazas internas y externas, donde las organizaciones deben tomar conciencia del valor de su información y la importancia de la privacidad de la misma.

Para mitigar la fuga de información, es necesario crear e implementar y monitorear una política de seguridad que contenga los estándares, procedimientos y guías para contrarrestar los efectos de un ataque de fuga de información.

Para realizar una política de seguridad de información, se debe tener claridad y compromiso de diferentes niveles corporativos directivos, comité de evaluación de políticas, proponente de la política generalmente debe ser el área de seguridad informática, usuarios y demás participantes directos e indirectos en la organización.

Una política de seguridad debe atravesar varias etapas de desarrollo, la cual inicia con su desarrollo, implementación, mantenimiento y eliminación, en las cuales intervienen distintos actores de la entidad, además de definir la responsabilidad de cada uno en cada etapa de la política.

De manera breve se mencionarán algunas actividades que se realizan en la creación de una política de seguridad de la información, como la planificación, investigación, documentación y coordinación de la política, evaluación y aprobación de la política por parte de los directivos, difusión, implementación, excepciones y concienciación de la política, seguimiento, mantenimiento y retiro de la política. [5]

F. Política de seguridad para dispositivos móviles

La política de seguridad para los dispositivos móviles en una entidad es fundamental para prevenir la fuga de información a través de estos medios, expuestos a diferentes vulnerabilidades y acceso fácil por extraños.

Para crear esta política es necesario contemplar los siguientes ítems:

- Sistema operativo que utiliza el dispositivo móvil.

- Los servicios corporativos a los cuales se accede desde el dispositivo.

- El control que tiene el usuario del hardware y software del dispositivo.

- Si la entidad tiene control remoto sobre el dispositivo.

Características de un dispositivo móvil.

Estas son algunas características que se deben evaluar en un dispositivo móvil:

- ¿Tienen reglas de firewall que podría establecer?

- ¿Cuándo puede desconectarse Bluetooth?

- ¿Cuán fuerte es el cifrado? No todos los dispositivos tiene el mismo cifrado fuerte.

- ¿Qué sucede cuando una determinada cantidad intentos con contraseñas fallan? ¿Se bloquea? ¿Se eliminan los datos?

Otros atributos a considerar son:

- ¿Qué permisos de aplicaciones puede habilitar o deshabilitar?

- ¿Qué tipo de entrada de datos del usuario? ¿Solo pantalla táctil, solo teclado qwerty o interfaz dual?
- ¿Qué tipo de servidor empresarial se utiliza para mejorar la política de seguridad para los dispositivos móviles?

Política seguridad para dispositivos Apple:

En esta clase de dispositivos como son iPhone y iPad el teclado físico no aplica, ya que cuando se activan algunas características como modo avión, deshabilita opciones inalámbricas ocasionando que no se pueda acceder desde un teclado externo.

La política puede establecer deshabilitar opciones comunes del dispositivo como son la cámara, archivos, instalar y desinstalar aplicaciones, así como eliminar información cuando se limite el número de intentos erróneos de ingreso de contraseña.

El administrador del servicio puede:

- Ajustar las configuraciones del dispositivo móvil.

- Consultar información del dispositivo para una lista de restricciones forzadas y una lista de instalación autorizada de aplicaciones en el dispositivo móvil.

- Administrar el dispositivo mediante la eliminación remota, el bloqueo remoto y la eliminación de la contraseña del dispositivo.

Políticas de seguridad para dispositivos Android:

Los dispositivos Android poseen varias opciones de acceso al usuario a través de teclados virtuales, teclados físicos y combinado.

En el dispositivo móvil con sistema operativo Android puede:

- Elegir un servidor empresarial Microsoft para el servicio corporativo de correo electrónico.

- Configurar los ajustes de bloqueo para evitar el uso no autorizado de su teléfono.

- Elegir la opción de mensajería móvil.

El administrador puede:

- Forzar el cifrado del dispositivo móvil, bloquear el dispositivo remoto, eliminar de forma remota la aplicación y los datos, la seguridad de la contraseña y las listas negras de los usuarios y de las aplicaciones.

- Instalar o desinstalar la aplicación de control, Bluetooth, Wi-Fi, la cámara y el micrófono.

- Configurar un cliente nativo de correo electrónico.

Políticas de seguridad para dispositivos RIM (Research In Motion - Investigación en movimiento limitado).

Los dispositivos RIM (BlackBerry) vienen en tres modos de entrada de datos:

- Teclado virtual, teclado qwerty y con interfaz dual, las opciones de seguridad incluyen la configuración de la contraseña, la instalación de la aplicación y el permiso, el firewall para bloquear los mensajes entrantes excepto los de direcciones específicas.

- Puede establecer una limpieza manual o automática de la memoria.

- Puede elegir encriptar los contenidos en tarjetas de medios solo por dispositivo, solo la contraseña o el dispositivo y la contraseña.

- Puede ajustar el dispositivo para evitar compartir los contenidos con dispositivos con Bluetooth.

- Encriptar datos que envía o recibe mediante la tecnología de Bluetooth.

- Evitar que otros utilicen la tecnología GPS para rastrear su ubicación.

También puede ajustar el dispositivo para conectarlo a un servidor empresarial de BlackBerry que pueda:

- Imponer restricciones de seguridad del dispositivo.

- Eliminar datos de un dispositivo perdido o robado.

- Imponer configuraciones de seguridad como bloqueos de Bluetooth.

Políticas de seguridad para dispositivos de Windows.

Los dispositivos móviles de Windows pueden tener acceso a un nivel o a dos niveles.

Un dispositivo con acceso a dos niveles tiene mejores opciones de permisos, como las que se ofrecen en Windows Mobile 6 y superior.

Restringe los permisos de inicio y el tiempo de ejecución de las aplicaciones. Una vez que se ejecuta una aplicación confirmada, los permisos de la aplicación, privilegiados y normales, son determinados por el certificado.

Si un usuario permite que se ejecute una aplicación sin confirmar, se ejecuta solo con los permisos normales. Sin embargo, el usuario podría no tener autorización para instalar las aplicaciones sin confirmar en un dispositivo móvil de dos noveles orientado a SaaS (Software as a Service). Se le podría pedir autorización para instalar las aplicaciones sin confirmar en un dispositivo móvil de dos noveles orientado a PaaS (Plataform as a service).

Necesita tener en su escritorio el gestor de configuración del dispositivo para cambiar las configuraciones de seguridad de su dispositivo.

Podría ser mejor incluir su dispositivo móvil a un servidor empresarial. Para permitir a los dispositivos móviles de Windows conectarse a un servidor empresarial de BlackBerry, necesita tecnología de conexión de BlackBerry.

Política de seguridad para dispositivos Symbian:

Los dispositivos Symbian (Nokia) tienen pantallas táctiles, teclados qwerty o un interfaz dual. La arquitectura de seguridad OS v9 de Symbian es personalizable y puede adaptarse para el uso de usuarios de dispositivos móviles, los operadores de red y los desarrolladores de software.

De forma subyacente a la Arquitectura de Seguridad OS v9 de Symbian hay dos controladores:

- Firewall para proteger los servidores clave del sistema.

- Encapsulamiento de datos para restringir las partes del sistema de archivos que están visibles para una aplicación o proceso específico.

Aunque la arquitectura de seguridad OS v9 de Symbian se encuentra disponible para proteger la serie 60 de la versión 9.x del sistema operativo de Symbian, podría ser mejor incluir su dispositivo móvil a un servidor empresarial. Para permitir a los dispositivos móviles de Symbian conectarse a un servidor empresarial de BlackBerry, necesita tecnología de conexión de BlackBerry.

La lista de verificación

Teniendo en cuenta lo anterior se observa que las políticas móviles varían de un dispositivo móvil a otro. Por ejemplo, los teléfonos BlackBerry tienen reglas de firewall explícitas, mientras que otros no. Una política de seguridad debe ser uniforme y aplicarse a todos los dispositivos móviles.

Para diseñar una esta política se debe elaborar la lista de verificación. Algunas claves para cada elemento de la lista de verificación, pueden ser:

- Propósito: ¿De qué se trata?

- Alcance: Escriba un límite en torno a la política.

- Trasfondo: ¿Quiere saber más?

- Acciones: Prepárese para el trabajo pesado.

Para lograr el objetivo de implementar la política de seguridad, se debe definir cuál es el propósito de la política de seguridad.

Propósito: ¿De qué se trata?

El propósito de la política consiste en ayudar a los proveedores de servicios empresariales a implementar la política de seguridad para:

Alcance: Definir el alcance de la política.

Defina el alcance al "incluir" un límite en torno a la política de seguridad. Dentro de sus límites, especifique qué dispositivos móviles se incluyen en la política.

El proveedor necesita descubrir si el consumidor permanecerá dentro del terreno (cumplirá con los términos de la política de seguridad sobre los controles de acceso, la protección de los datos y la gestión virtual de las máquinas). Si el consumidor se retira del terreno después de acordar cumplir, el usuario de dispositivo móvil corre el riesgo de violar la política. En este caso, el proveedor debe indicar las consecuencias de no cumplir para asegurarse de que el consumidor se mantenga dentro del terreno.

Trasfondo: Lo que se encuentra detrás de la política

Lo primero que quiere saber un consumidor es si el proveedor es interno o externo y cuáles son los límites de gestión de controles entre el proveedor y un usuario de dispositivo móvil cómo administraría el proveedor los controles de acceso, proporcionaría la protección de datos y gestionaría máquinas virtuales, y respondería a los ataques de seguridad en la nube o los incidentes en los dispositivos móviles.

Acciones: Sugerencias de acciones a realizar.

A continuación se incluyen cinco sugerencias para acciones para que los clientes estén contentos:

- Acción 1. Envío de copias a los consumidores de la política de seguridad y preguntas a resolver antes de que el consumidor se registre para obtener un

servicio en la nube al acceder desde su dispositivo móvil.

- Acción 2. Establecimiento de las normas de firewall.

- Acción 3. Hacer que los consumidores se adhieran a un servidor de gestión de dispositivos empresariales.

- Acción 4. Permitir que los desarrolladores de aplicaciones de la PaaS y sus usuarios del SaaS se suscriban a una aplicación corresidente del SaaS.

- Acción 5. Especificar qué aplicaciones se instalen o desinstalen en los dispositivos móviles registrados con el servidor de la empresa. [5]

III. CONCLUSIONES

En base con lo analizado del artículo, es necesario concientizarnos del riesgo que corremos, al no implementar correctamente las políticas de seguridad de la información y no proteger los dispositivos móviles con la instalación de antivirus y anti spam, al interactuar con los datos empresariales, nos convertimos en un medio facilitador para los ataques de los cibercriminales.

De igual forma las empresas creadoras de antivirus se han enfocado en desarrollar herramientas para bloquear y hacer limpieza de todos los virus, gusanos, troyanos y demás programas que detectan los motores de antivirus, esto para reducir el riesgo de fuga de información de las empresas por medio de nuestros dispositivos móviles y equipos de cómputo.

Así mismo, es importante que nos concienticemos de las vulnerabilidades que tenemos en la red y en nuestros dispositivos, que nos demos cuenta del valor de la información tanto empresarial como personal y sobre todo la responsabilidad que poseemos sobre la misma.

REFERENCIAS

[1] https://www.sophos.com
[Online] "Proteja sus dispositivos móviles."
www.support.godaddy.com
[Online] "Como identificar eliminar y prevenir código malicioso en su servidor de alojamiento."

[2] http://www.eset-la.com
[Online] "Tendencias 2014 El desafío de la privacidad en Internet."
https://www.symantec.com
[Online] "Tendencias de seguridad cibernética en américa latina y el caribe."

[3] http://www.ccp.gov.co
[Online] "Boletines ciberseguridad"

[4] http://www.welivesecurity.com
[Online] "10 años de fuga de información: conoce los incidentes para no repetir la historia."

[5] http://www.redseguridad.com
[Online] "Fuga de información, la mayor amenaza para la reputación corporativa"
http://www.mintic.gov.co
[Online] "Formato e implementación de políticas de seguridad y privacidad de la información"

[6] http://www.ibm.com
[Online] "Modelado de política de seguridad para dispositivos móviles"

Jose Parmenio Bravo Bermejo. Ingeniero de Sistemas, "Especialización en Seguridad Informática" Universidad Piloto de Colombia 2015.