Recomendaciones de seguridad para Dispositivos Portátiles y Smartphones

www.securizame.com

19 de Febrero de 2014

1. Indice

2. Presentación

"Comunicaciones y Seguridad de la Información, S.L.", en adelante Securízame, es una empresa sustentada en 13 años de experiencia profesional por parte de sus integrantes, en grandes y medianos proyectos de seguridad informática, peritaje y formación.

Securízame cuenta en su plantilla con profesionales especializados en seguridad informática, ponentes en Congresos Nacionales e Internacionales, y con amplia experiencia en formación reglada en seguridad informática. Además, trabaja en estrecha relación con partners reconocidos en el sector de la auditoría y consultoría de seguridad.

Securízame lleva a cabo proyectos en importantes clientes de la industria nacional y multinacional. Como referencias podemos destacar las siguientes:

- Ilustre Colegio de Abogados de Guadalajara
- Estructuras de Venta Directa / Grupo de Mercados Telemáticos
- Yoigo
- Ayuntamiento de Guadalajara
- Diputación de Guadalajara
- Abogados Martínez-Sarralde Asociados
- eTaxi
- ISDelgado
- Tribunal Constitucional de España
- EXIDE
- APYCE, Gestión de la comunicación
- Oxford University Press
- Consultec
- Diximedia
- Torresol Energy
- Grupo Caamaño
- Invías: Instituto Nacional de Vías de Colombia
- Valeo
- Instituto de Desarrollo Urbano IDU en Colombia
- PCMancha
- INTECO
- RIU Hotels & Resorts
- RebajasVIP
- Grupo de Delitos Telemáticos Guardia Civil
- Diario Online El Confidencial

3. Alcance del documento

<El Cliente>, empresa concienciada de la sensibilidad de la información existente en sus dispositivos móviles (ordenadores portátiles, tablets y smartphones), ha encargado a Securízame, empresa especializada en servicios de seguridad informática y comunicaciones, el desarrollo del presente documento con medidas de mejora de la seguridad de los mismos.

El presente documento pretende dejar constancia de diferentes medidas de seguridad tecnológicamente viables para mejorar la seguridad de los dispositivos móviles propiedad de <El Cliente>, así como de los mecanismos de conexión remota existentes.

El resto de medidas de seguridad complementarias, relativas a concienciación a usuarios ante la actitud a tener ante situaciones tales como la conexión de redes inalámbricas públicas, la ejecución o apertura de ficheros de fuentes no confiables, el acceso a enlaces acortados, URLs no necesarias para su trabajo, etc, etc,… quedan fuera del presente documento.

4. Recomendaciones de seguridad comunes

Tanto para ordenadores portátiles como para tablets y smartphones, las recomendaciones comunes a tener en cuenta son las siguientes:

4.1 Gestión centralizada de equipos

Una de las mejores formas de tener controlado el parque de equipos móviles (ordenadores portátiles como dispositivos móviles) es que todos los equipos estén inventariados en una misma plataforma. Existe en el mercado soluciones de gestión MDM (Mobile Device Management) que permiten registrar el estado de cada uno de los mismos, tanto para obligar una política común a todos ellos (o incluso diferentes políticas dependiendo de una clasificación por grupos) como para monitorizar si alguno de ellos incumple las directrices estipuladas por la organización.

4.2 Maquetado homogéneo

Derivado de la recomendación anterior, para llevar a cabo una correcta gestión, el maquetado de todos los dispositivos móviles y ordenadores portátiles, deberá ser el mismo. La instalación del sistema operativo deberá contar con los mínimos requisitos de servicios software posibles. Esto implica el sistema operativo en su mínima expresión. A partir de ahí, se evaluarán los complementos necesarios para trabajar: Máquina Virtual Java, Plugins Adobe como Flash, Shockwave, codecs de video, etc,…

4.3 Selección de software seguro

Si se puede elegir el software a instalar, siendo que varias soluciones permitan llevar a cabo la misma funcionalidad, como por ejemplo podría ser permitir el acceso a documentos PDF, se recomienda la selección de software que, aun no siendo muy conocido, sea igualmente compatible y que no esté "en el punto de mira permanente". Es decir, que se evite la utilización de software más proclive a que existan exploits públicos o 0-Day ante vulnerabilidades, por lo altamente extendido, a nivel estadístico, del software.

4.4 Instalación desde medios originales

Tanto la instalación del sistema operativo, como del software seleccionado, deberá ser llevada a cabo desde medios físicos (CDs/DVDs) originales, o copias de estos. Cuando se instale software descargado de Internet, deberá hacerse con las debidas garantías de la fuente del mismo. Esto es, que sea descargado de la web del fabricante directamente evitando páginas de software pirata con "cracks" adjuntos.

4.5 Contraseña de arranque

Para ordenadores portátiles, se habilitará la contraseña para arranque en BIOS (si es posible). En caso contrario, se recomienda la implantanción de alguna solución software de cifrado de disco que exija una contraseña fuerte en pre-boot. Este impide el acceso a

la información sensible por el cifrado y además para el arranque. En el caso de teléfonos móviles y tablets, se hace imprescindible la utilización de un PIN o contraseña que impida el acceso al dispositivo.

4.6 Política de contraseñas

Para ordenadores portátiles, lo recomendable es que los usuarios pertenezcan al dominio Microsoft existente en la organización, con políticas de complejidad y caducidad adecuadas, así como con "memoria" de las últimas cinco contraseñas anteriores de cada usuario.

En el caso de teléfonos móviles/tablets, el PIN o contraseña del dispositivo debe, al menos, existir. En el caso de dispositivos Android, deben evitarse los controles de acceso basados en patrones de puntos, siendo lo más deseable el control biométrico por huella dactilar, en aquellos dispositivos que lo soporten. En caso que sea necesario un PIN o contraseña, se recomienda forzar teclado alfanumérico, y cierta complejidad en la contraseña exigiendo letras minúsculas, mayúsculas y números, así como el bloqueo temporal según se va fallando en la autenticación. En algunos dispositivos con información muy sensible, podría activarse incluso el check de borrado completo del dispositivo si hay 10 fallos seguidos en la autenticación.

4.7 Bloqueo de sesión por inactividad

Tanto en ordenadores portátiles como en smartphones y tablets, habrá de activarse las políticas de bloqueo de sesión (o de apagado de pantalla) solicitando autenticación o PIN para volver a interactuar con el dispositivo. El periodo máximo de inactividad antes de dicho bloqueo se recomienda que se fije en 1 minuto para smartphones y tablets, así como 3 minutos para ordenadores portátiles.

4.8 Filtros de privacidad

Los dispositivos móviles objeto de securización de esta guía pueden usarse en lugares públicos como aviones, trenes, cafeterías, etc,… en los que los ojos ajenos de personas cercanas pueden interesarse por la información que aparece en la pantalla. Para evitar esto, se recomienda la utilización de un filtro de privacidad integrado (pegado de forma permanente) en el monitor o en la pantalla del smartphone o tablet. Esto permite que lo mostrado en la pantalla sólo sea visible de frente, esto es por el usuario del dispositivo, protegiendo de extraños que miren desde cualquier otro ángulo.

4.9 Tapar físicamente las cámaras integradas

El malware de hoy en día permite activar la webcam incorporada en dispositivos móviles a voluntad del atacante, por lo que es posible disponer de una cámara y un micrófono de forma remota, escuchando y viendo al usuario. A fin de proteger la privacidad del usuario, así como de la información hablada por su parte (y que pueda ser monitorizada en remoto, a través del micrófono), se recomienda bloquear físicamente la webcam con cinta aislante negra, con la opacidad necesaria para que no

se pueda ver nada. Igualmente, en ordenadores portátiles, se recomienda aplicar un punto de cinta aislante en el micrófono incorporado en el equipo.

Si el dispositivo corporativo requiere utilización para videoconferencias, existen dispositivos que permiten tapar la webcam de un ordenador de forma selectiva sin usar cinta aislante, bloqueando la señal visual captada por la misma. Estos dispositivos se llaman iPatch (http://www.ipatchweb.com/en/)

4.10 Cifrado de dispositivo

Como se ha indicado en puntos anteriores, para ordenadores portátiles, se recomienda utilizar un sistema de cifrado en pre-boot, que pida una contraseña de acceso y descifrado del disco duro. De esta manera, en caso de pérdida o robo, no servirá para nada extraer el disco duro y montarlo desde otra plataforma puesto que el mismo estará cifrado completamente. En Apple, la opción nativa es Filevault y en Microsoft, Bitlocker. En portátiles con Microsoft Windows, puede utilizarse Truecrypt como alternativa, aunque es recomendable Bitlocker por estar soportada por Microsoft de forma corporativa. En caso que no se desee hacer un cifrado completo del disco, al menos será altamente recomendable que la información tratada en local se guarde en un contenedor cifrado. Para este fin, se recomienda la utilización de soluciones como Truecrypt, compatible con sistemas operativos Windows, Mac y Linux.

En dispositivos móviles Apple, la información está cifrada a nivel hardware y su acceso libre depende o no de la existencia de PIN o contraseña de desbloqueo.

En dispositivos móviles Android, el cifrado es opcional, y se recomienda que tanto para la flash del dispositivo como para los datos contenidos en la tarjeta SD externa, se active la opción de cifrado existente.

4.11 Gestión de contraseñas

A lo largo del día a día, los usuarios utilizan diferentes credenciales de autenticación para acceso a datos sensibles. Dada la cantidad de credenciales, si además se cumplen los requisitos de complejidad, y los usuarios utilizan diferentes pares usuario/contraseña para cada servicio, se hace muy difícil acordarse de todas. Para evitar que los usuarios tengan apuntadas las contraseñas, tanto en papel como en texto claro, se recomienda utilizar un gestor de contraseñas. Esta solución almacena de forma cifrada tantas credenciales como se desee. Además, permite tanto generar como recordar contraseñas de forma segura, haciendo que el usuario ni siquiera tenga que sabérselas. La solución recomendada es KeePassX.

4.12 Actualizaciones de software

Tanto para ordenadores portátiles, como para smartphones y tablets, siempre es recomendable disponer del software instalado a último nivel de actualización, puesto

que los fabricantes, además de nuevas funcionalidades, corrigen fallos de aplicación y aplican parches de seguridad.

A menudo, la propia operativa de los fabricantes, así como las diferentes versiones de máquinas sobre las que se instala el software, puede que haya problemas de incompatibilidad con determinado hardware. Además, no sería la primera vez que la publicación de un parche inutiliza otras funcionalidades del software o del sistema operativo, incluso dejándolo inservible. Dicho esto, no se recomienda la aplicación de los parches o últimas versiones de sistema operativo según ésta son publicadas en todo el parque de dispositivos, sino que se sugiere dar un margen de tiempo aceptable con el que se monitorice que el parche es estable. Igualmente, lo recomendable es la aplicación del mismo en un dispositivo de prueba (tanto para smartphones, tablets como portátiles) de manera que se pueda garantizar que la aplicación del parche/actualización no interfiere con el software actualmente instalado.

Una vez se hayan hecho las comprobaciones adecuadas, se puede instalar de forma centralizada y global la actualización en todos los dispositivos, lo antes posible, a fin de minimizar la ventana de exposición vulnerable.

4.13 Herramientas de Tracking y borrado remoto

Ante la pérdida o robo de un dispositivo, a fin de poder recuperarlo o de identificar la ubicación actual del mismo, se recomienda la instalación de software que permita estos cometidos. En teléfonos móviles y tablets, incluso se utiliza el GPS integrado del equipo para poder ayudar a determinar la ubicación. En el caso de ordenadores portátiles, cuando el equipo es conectado a Internet, envía una señal a una central desde la que se puede incluso utilizar la webcam del equipo, para poder identificar al actual poseedor del mismo. Una de las más conocidas es Prey (http://www.securitybydefault.com/2012/01/prey-quien-ha-robado-mi-queso.html)

4.14 Provisioning redes Wifi y VPN

Tanto para el acceso a redes inalámbricas corporativas con credenciales de autenticación como para el acceso por VPN, se recomienda que vengan pre-configuradas a nivel de maqueta, tanto en ordenadores portátiles como en smartphones y tablets. De esta manera, se hace transparente a los usuarios el conocimiento de determinadas credenciales (que luego puedan compartir con otros usuarios/dispositivos no autorizados), así como por transparencia y comodidad para los mismos.

5. Recomendaciones de seguridad para ordenadores portátiles

Para ordenadores portátiles, las recomendaciones comunes a tener en cuenta son las siguientes:

5.1 Contraseña en acceso a BIOS

En todos los modelos que sea posible, el acceso a la BIOS del ordenador debe estar protegida mediante un acceso con PIN/contraseña, únicamente conocido por el departamento de sistemas de la organización. Esto evitará que se puedan hacer cambios en las configuraciones de seguridad que se apliquen a nivel BIOS, como puede ser determinar el orden de los dispositivos de arranque, deshabilitar los dipositivos USB (en aquellas BIOS que así lo permitan), etc,…

5.2 Deshabilitar medios externos

Desde el punto de vista de DLP (Data Loss/Leak Prevention), así como de entrada de malware se recomienda limitar determinados puntos de entrada/salida de datos. Entre otros, se encuentran: Lectores de CD, conectores USB, tarjetas SD, etc,… La recomendación es que por defecto estén deshabilitados en todos los equipos, excepto en aquellos que sean estrictamente necesarios.

5.3 Usuarios no-privilegiados

Para acotar aún más el daño que pueda realizar un malware en un sistema, se recomienda que la ejecución de cada programa, se haga limitando a la utilización de usuarios no-privilegiados (es decir, sin privilegios de administrador). Dado que los ordenadores portátiles de la organización forman parte de un dominio Microsoft, se recomienda revisar la existencia de usuarios que sean administradores locales en los ordenadores, y su inmediata eliminación, siendo el único acceso permitido mediante usuarios de dominio, no privilegiados.

5.4 Software instalado (lista blanca)

Dado que las necesidades de software a utilizar por la organzación son conocidas, se recomienda instalar el software permitido y prohibir, por políticas de dominio, a los usuarios que puedan instalar software en los ordenadores portátiles. Así se evitará la entrada de cierto malware por poca fiabilidad de las fuentes de instalación del software elegido por el usuario, como posibles problemas legales por disponer de software sin licencia.

5.5 Antimalware corporativo

Se recomienda que todos los equipos dispongan de un antimalware corporativo, actualizado a última versión de firmas con frecuencia diaria. El antimalware elegido, se recomienda que disponga de una consola centralizada de administración y monitorización de agentes. Si existe en la organización algún sistema de análisis de

malware a nivel de gateway (o de proxy) de algún fabricante, se sugiere que el antimalware elegido para cada EndPoint sea de un fabricante diferente (de una primera marca).

5.6 Conexión VPN obligatoria

Para poder acceder a recursos internos de la organización, se recomienda que la única forma permitida de acceso sea mediante un túnel establecido por VPN. Las características de seguridad del mismo deberían incluir cifrado mediante algoritmo AES-256, hashing SHA1 (por compatibilidad con sistemas operativos de smartphones y tablets), autenticación mediante certificados digitales y Xauth, exigiendo usuario y contraseña integrada con el dominio o con algún sistema OTP (One-Time Password) basada en aplicación, SMS, Token, etc,…

En el servidor VPN se deberá activar el setting “All Traffic”, para que la ruta por defecto del equipo sea el gateway VPN, forzando que todo el tráfico pase a través del túnel.

Si a esto se suma la navegación forzada a través de proxy, existente en un direccionamiento interno, se dispondrá de los mismos controles de seguridad en la navegación de cualquier dispositivo ubicado físicamente en las dependencias de la organización.

6. Recomendaciones de seguridad para teléfonos móviles y tablets

Tanto para tablets como para smartphones, las recomendaciones comunes a tener en cuenta son las siguientes:

6.1 No Jailbreak/Rooteo

Por coherencia con la recomendación común de instalación de software original, se recomienda no efectuar "jailbreak" o "Rooteo" de smartphones ni tablets. Los fabricantes de dichos dispositivos introducen, en sus firmwares originales, restricciones de control de instalación de software no firmado o no autorizado. De esta manera se mitiga el riesgo de ejecución de algunos tipos de malware.

Al efectuar jailbreak, se eliminan dichas restricciones, de manera que es posible instalar aplicaciones no originales, crackeadas o troyanizadas.

Tanto desde un punto de vista de seguridad, como de cumplimiento legal con las licencias de software, se recomienda mantener el firmware original y a último nivel de actualizaciones de seguridad originales.

6.2 Antimalware corporativo (Android)

En el caso de dispositivos Android, donde la cantidad de malware existente es mayor, se recomienda la integración de un antimalware centralizado y corporativo para todo el parque de tablets y smartphones.

6.3 Posibilidad de borrado remoto

Aunque ya se ha comentado en recomendaciones globales, la existencia de soluciones para borrado remoto y para tracking de equipos, en el caso de dispositivos móviles tiene mayor énfasis debido a la mayor facilidad de pérdida de los mismos, así como de las capacidades de localización gracias al GPS integrado.

En el caso de dispositivos IOS, Apple incorpora las funcionalidades de tracking y de borrado remoto, gracias a la integración con iCloud, mediante "Find My Iphone"

7. Licencia de este documento

El presente documento se ha licenciado, para su libre distribución, con licencia Creative Commons con las siguientes características:

- Reconocimiento de la autoría
- No se permite la comercialización de la obra original ni derivadas
- Si se distribuye hay que hacerlo con una licencia igual