Pequeño Negocio, Gran Amenaza

Mejores Prácticas de Seguridad para Dispositivos Móbiles

Antecedentes e Introducción

El propósito del siguiente documento es para ayudar a su negocio a tomar las medidas necesarias para utilizar las mejores prácticas de seguridad para usted y para los dispositivos móviles de sus empleados.

Este documento discute las prácticas de seguridad más básicas que **TODOS** deberían seguir como punto de partida. Si usted siente que pertenece a una categoría más compleja, es altamente recomendable que contacte a su proveedor de IT para futura dirección y asistencia.

Esta no es una lista comprensiva de todos los posibles procedimientos de seguridad, como muchas de las necesidades más avanzadas de IT dependen de la naturaleza del negocio y si el negocio tiene que cumplir con requerimientos de conformidad con su industria

Principales Amenazas en contra dispositivos móviles

- **Pérdida de datos**
  Un empleado o hacker teniendo acceso a información sensible desde un dispositivo o red. Esto puede ser involuntario o malicioso y es considerado la mayor amenaza a dispositivos móviles.

- **Ataques usando ingeniería social**
  Un cyber criminal intenta engañar a los usuarios para que revelen información sensible o para que permitan la instalación de malware. Métodos incluyen suplantación de identidad (phishing), suplantación de identidad usando mensajes de texto (SMishing) y ataques específicos.

- **Malware**
  Software malicioso que incluyen virus tradicionales, gusanos informáticos y troyanos (Trojan horse programs). Ejemplos específicos incluyen el gusano informático Ikee, ataques a dispositivos basados en iOS; y Pjapps malware que pueden registrarse en dispositivos Android infectados en una colección de hacker controlados “zombie” dispositivos conocidos como “botnet.”

- **Amenazas a la Integridad de datos**
  Intentos de corromper y modificar datos con el objetivo de interrumpir las operaciones de un -

negocio para tener ganancias financieras. Esto puede ocurrir también involuntariamente.

- **Abuso de Recursos**
  Intentos de mal uso de las redes, dispositivos o recursos de identidad. Ejemplos incluyen envío de correo no deseado desde dispositivos comprometidos o negación de los ataques de servicios usando recursos informáticos desde dispositivos comprometidos.

- **Ataques basados en la web y las redes**
  Lanzados por páginas web maliciosas o sitios comprometidos, estos atacan al navegador en un dispositivo e intentan instalar malware o robar datos confidenciales que fluyen a través del navegador.

Cuando considere el uso de dispositivos móviles, considere lo siguiente:

- ¿Cómo estos dispositivos móviles están siendo usados desde una perspectiva personal y de negocio?
- ¿Qué limitaciones se necesitan imponer en el uso de dispositivos móviles en la compañía usando políticas y cumplimiento?
- ¿Cómo podemos monitorear las redes para asegurar que las políticas están siendo cumplidas?
    - Asegúrese que las políticas son adaptadas a los dispositivos específicos de sus empleados, roles y lugares.

Mejores Prácticas

- **Elija Dispositivos Móbiles cuidadosamente**
  No todos los dispositivos han sido fabricados iguales cuando hablamos en términos de seguridad. Por ejemplo: iPods fueron fabricados para consumo general sin preocupaciones acerca de seguridad y por lo tanto fueron menos seguros que un dispositivo BlackBerry diseñado para usuarios especiales como cumplidores de la ley; Los teléfonos inteligentes de Android y Apple han sido diseñados para ser bastante seguros pero no al mismo nivel que los dispositivos de BlackBerry. Comunique a sus empleados cuales son los dispositivos que la compañía da soporte y también cuales autoriza a tener acceso a la información de la compañía, e instrúyalos en los procedimientos requeridos para que sean instalados apropiadamente. En muchos de los casos es recomendable que la empresa tenga un profesional en dispositivos móviles para realizar la instalación a menos que la compañía tenga un experto.

- **Actualice el software de los dispositivos móviles y las aplicaciones móviles**
  La mayoría de las aplicaciones de los dispositivos móviles y sistemas operativos proveen notificaciones cuando las actualizaciones son requeridas; adicionalmente muchos de los dispositivos móviles le permiten configurar el teléfono para que las actualizaciones sean implementadas

automáticamente, sin necesidad de tomar acciones extras, es óptimo. De esta manera el sistema operativo y aplicaciones móviles siempre estarán actualizadas (incluyendo cualquier actualización de seguridad que los desarrolladores de aplicaciones han implementado) para estar lo más protegido como sea posible.

- **Instalación de Anti-malware software en dispositivos móviles**
  Nuevas amenazas malware dirigen sus ataques a sistemas operativos como iOS (Apple/iPhone) y Android (Google) y son descubiertos y explotados todos los días. El software de seguridad también debe ser actualizado y mantenido como cualquier otro software. Las políticas de la Compañía deben asegurarse que esto es un requerimiento mandatorio para todo empleado que usa dispositivos móviles para el negocio; sean estos dispositivos de propiedad personal o del negocio. Si van a acceder a los datos de la empresa, la instalación de un software anti-malware **aprobado** deberá ser un requerimiento.

- **Toda la comunicación de los dispositivos móviles DEBE estar encriptada.**
  Hoy la comunicación inalámbrica [Wi-Fi] es fácilmente interceptada permitiendo que los datos sean robados o manipulados, por lo tanto es imperativo que todos los empleados utilicen encripción en todas las comunicaciones de texto y todo tipo de datos en los dispositivos móviles. Busque profesionales en tecnología para dirección en conseguir esto y para que provea el entrenamiento necesario a su personal.

- **Las Políticas de la compañía deben requerir autenticaciones y contraseñas fuertes**
  Algunos de los nuevos dispositivos móviles incluyen opciones de seguridad local construidos en biometría – escáneres de huellas dactilares, reconocimiento facial, reconocimiento de voz impresa y mucho más; cuando sea posible se deberá insistir que estas opciones sean utilizadas. En la ausencia de estas nuevas opciones es imperativo que se utilicen fuertes autenticaciones y contraseñas y que la instalación asegure posesión del dispositivo móvil no garantice acceso a información importante y al sistema tampoco. Otra vez, tenga la certeza de que sus empleados escojan la contraseña más fuerte que el dispositivo permita.

- **Planifique para lo peor – dispositivos perdidos o robados**
  En adición a las mejores prácticas señaladas en la parte posterior, es recomendable que a los dispositivos móviles de la compañía se les pueda borrar toda la información almacenada en caso de pérdida o robo. Esto ayudará a prevenir el acceso a los datos en este tipo de situaciones. Existen sistemas de manejo de móviles disponibles que proveen este tipo de competencias, el software de seguridad en muchos de los dispositivos móviles proveen esta competencia o como recurso final los proveedores de servicios móviles lo pueden implementar (pero no espere que el proceso con ellos sea fácil o rápido, y más probable costoso).

- **Software de terceros [aplicaciones]**
  Las políticas de la compañía deben limitar o bloquear el uso de software de terceros en dispositivos provistos por la compañía. Esta es la mejor manera de prevenir posibles compromisos y fallas de seguridad, resultando en el intento de instalación de drives o software deshonesto (rogue software),

lleno de backdoors y "black gateways" para desviar la información. Desafortunadamente, no existen opciones si sus empleados están usando sus dispositivos personales para el trabajo. En el caso de dispositivos provistos por la compañía se sugiere que se provea una lista de aplicaciones móviles pre aprobadas, verificados que se podrían utilizar en los dispositivos de la compañía para mantener los riesgos de software de terceros en lo mínimo. Si necesita asistencia con la verificación de aplicaciones seguras para el uso aprobado por el personal de la compañía, contacte la asistencia de un profesional en tecnología.

- **Cree separado, mobile gateways seguros**
  Sea diligente y comprenda a fondo que tipo de usos, sistemas, y aplicaciones, los usuarios de dispositivos móviles de su firma requieren acceso y usan. Provea de un específico gateway para acceso que está protegido con el software anti-malware más actualizado y otras herramientas de cyber seguridad. Estas herramientas deberán incluir aplicaciones de prevención de pérdida de datos y filtro de contenido. Muchas empresas pequeñas no tienen el conocimiento técnico para implementar esto, por lo que deben adquirir los servicios de un profesional en tecnología bien respetado (no su sobrino de colegio o su cuñado que tomó clases de programación y está seguro de lo que se debe hacer)

- **"Bloqueo" de todos los dispositivos móviles es obligatorio**
  Las políticas de la compañía requiere que antes que se autorice a los empleados el uso de dispositivos móviles, estos deben ser configurados para evitar el uso de redes inalámbricas inseguras, y el Bluetooth debe estar escondido para evitar el descubrimiento del mismo. Cuando el uso de auriculares y audífonos no es active el Bluetooth deberá ser deshabilitado conjuntamente. Otra vez, en muchos casos se necesita emplear el uso de un profesional de tecnología para configurar los dispositivos de los empleados; también se deben realizar auditorías sorpresas periódicamente a los dispositivos de los empleados usando tecnología profesional para asegurar que los empleados no cambien la configuración y pongan los datos en riesgo. Los empleados deben requerir permiso para estas auditorías para que se les permita el uso de teléfonos personales para los negocios de la compañía.

- **Ejecute auditorías regulares de seguridad móvil incluyendo pruebas de penetración [pen-testing]**
  Estas auditorías deberán realizarse al menos una vez al año. Es recomendable que las compañías contraten a una firma acreditada para la prueba de seguridad para la auditoría de la seguridad de los dispositivos móviles. Estas firmas podrán ayudar con remediación y mitigación de cualquier problema que se ha descubierto.

  ****Prueba de penetración*** es proactiva e intento autorizado para evaluar la seguridad de la infraestructura de IT con un intento seguro de explotar las vulnerabilidades del sistema incluyendo: el sistema operativo (OS), fallas de servicios y aplicaciones, configuraciones no apropiadas y hasta comportamiento riesgoso por parte del usuario final. Tales evaluaciones son muy útiles para validar la eficacia de los mecanismos de defensa, así como la adherencia a las políticas de la empresa por parte de los usuarios finales.

Pequeño Negocio, Gran Amenaza

- **Control del uso de la batería en los dispositivos móviles**
  Note cuanto tiempo dura la batería. Si nota un cambio significante en la disminución de la vida de la batería, a veces malware puede ser la causa de esta disminución y deberá tener un profesional examinando su dispositivo lo más pronto posible – y absténgase del uso del dispositivo hasta que se haya determinado que está limpio, esto ayuda a minimizar el riesgo de que hackers ganen acceso a los datos de la compañía.

- **No use Wi-Fi público**
  Wi-Fi público es fácilmente violado y por lo tanto es usado a menudo por hackers, quienes aparentan estar muy ocupados trabajando en la cafetería cerca a los empleados – y pueden estar muy ocupados trabajando – robando la información de la compañía a través del celular o tableta del empleado! Instruya a los empleados a evitar el uso de Wi-Fi público bajo toda circunstancia.

- **EDUQUE, EDUQUE, EDUQUE**
  La seguridad de dispositivos móviles deberá complementar y ampliar las políticas de cyber seguridad por parte de IT. La participación en la educación de cyber seguridad deberá ser un requerimiento a todos los empleados. Explique exactamente como los dispositivos son entregados, y que configuraciones y aplicaciones están permitidas. Diga, indique, póngalo por escrito!!! Si no siente cómodo ofreciendo esta educación, utilice servicios de un profesional de tecnología, y si es necesario grabe en video para que pueda ser usado en las futuras contrataciones.

- **Actualizaciones**
  Asegúrese de borrar toda la información de los dispositivos móviles que serán re-usados o devueltos al proveedor para ser actualizados. Borrando el contenido del dispositivo no es suficiente; siga las instrucciones del dispositivo para devolverlos al sistema original del fabricante. Si no puede encontrar la información; pregunte a su proveedor o contrate un profesional para que lo haga por usted, de otra manera datos pueden permanecer en el dispositivo sin que usted se dé cuenta. Esos datos pueden comprometer su firma y/o la personal que previamente utilizo el teléfono **NOTA:** Jailbroken, rooted, non-manufacturer ROM-based dispositivos talvez no respondan al comando de borrado.

- **Evite abrir inesperados mensajes de texto de remitentes desconocidos**
  Una de las nuevas maneras de comprometer dispositivos móviles es SMSishing (o SMS phishing – busque la definición en el doc Q&A). Esta forma de ataque es cuando un potencial ladrón de identidad envía un mensaje de texto preguntando por información personal de la cuenta. Esta información puede ser usada para acceder a los sistemas corporativos, banca, cuentas financieras así como para el envío de malware. SA veces el dispositivo es comprometido y el dueño es víctima de “rescate” (ransomware). Como el término sugiere, el dispositivo es bloqueado y el dueño debe “pagar un rescate” para obtener acceso.

- **No abra correos electrónicos dudosos**

Pequeño Negocio, Gran Amenaza

No abra correos electrónicos que se vean dudosos – ni siquiera si parece que el correo electrónico viene de un contacto que es familiar. Los contactos de esa persona pueden haber sido hackeados y los hackers están utilizando el correo electrónico de esa persona y todos sus contactos para el envío de virus. Esté muy alerta observando errores de ortografía en la línea de asunto, gramática extraña, uso de mayúsculas en la línea de asunto o algo más que parezca inusual. NUNCA dé un click en un enlace a menos que esté completamente seguro que es de una fuente segura.

- **Posesión es la pregunta**
  ¿Los empleados estarán autorizados a usar dispositivos móviles personales para los negocios de la compañía o la compañía les proveerá dispositivos para uso exclusivo para los negocios? Negocios que proveen dispositivos móviles a sus empleados tienen una gran oportunidad de mantener su información segura.

- **Las redes sociales requieren precaución**
  Sea muy precavido al acceder a enlaces, videos, fotos, códigos QR, etc. desde las redes sociales; no es difícil para los hackers adjuntar virus y malware en cualquiera de los contenidos de las redes sociales populares donde ellos se aseguran que los mismos estén escondidos en los tópicos más populares y estos son abiertos y compartidos cientos y miles de veces y como la mayoría de usuarios acceden a las redes sociales a través de las redes sociales, esta vía les provee fácil y rápidos acceso a cientos y miles de dispositivos móviles.

Pequeño Negocio, Gran Amenaza

Seguridad Móvil – Un estado de la mente

La seguridad de dispositivos móviles es tan solo una fracción de la infraestructura de seguridad, el dueño de la empresa debe asegurarse de tenerla para proteger a los empleados, los activos, la reputación de la empresa y la visión del negocio. Se deberá tomar las medidas necesarias para mitigar (reducir) los riesgos y prevenir pérdidas permitiendo a empresarios, contratistas y empleados a tomar ventaja de los dispositivos móviles en el lugar de trabajo. Recuerde el fracaso puede dar lugar a responsabilidades legales, multas y/o pérdida de negocios.

Manejo de "Traiga su propio dispositivo" "Bring Your Own Device" [BYOD] (lo que significa que los empleados usen sus propios dispositivos móviles para trabajar) para una compañía requiere el aprendizaje de ambientes virtuales de trabajo como "VPNs" o Virtual Private Networks (Redes Virtuales Privadas). Estos sistemas autónomos autorizan a los empleados a trabajar remotamente mientras acceden a sistemas limitados, aplicaciones e información. Para más información detallada acerca de VPNs, contacte a un profesional de cyber seguridad de confianza.

Un recurso de confianza para la creación de Políticas de Dispositivos Móbiles para su compañía lo puede encontrar en este enlace – http://www.sans.org/reading-room/whitepapers/pda/security-policy-handheld-devices-corporate- environments-32823