ZEBRA

ESTABLECIENDO UNA PÓLIZA ROBUSTA DE SEGURIDAD MÓVIL: Los riesgos principales y cómo las empresas pueden evitar dichas prácticas.

A menudo, la seguridad de TI de movilidad empresarial es comparada a un seguro y usualmente se tiene en cuenta porque es una necesidad. Sin embargo, con esa visión limitada se pierde lo esencial. La seguridad provee más que sólo el cubrimiento en respuesta a un evento específico. También ofrece una garantía – lo que le permite a su empresa operar e innovar sin el riesgo de brechas de datos.

En este documento técnico, exploramos cuales son las consideraciones claves para el desarrollo de una póliza robusta de seguridad móvil. Presentamos los riesgos principales y lo que puede hacer acerca de ellos para poner en marcha nuevas oportunidades para mejorar la productividad, eficiencia y exactitud en todas sus operaciones.

No existe un enfoque uniforme

Siguen existiendo algunas diferencias de opiniones sobre la necesidad de la seguridad. Aún, todos pueden estar de acuerdo que se trata de un tema complejo que afecta a muchas áreas de la organización. La necesidad global de la seguridad, así como la complejidad, es más evidente cuando se considera la variedad en casos de uso de movilidad, metodologías de aplicaciones y opciones de implementación de las empresas individuales.

En las tiendas de retail, los empleados con tabletas pueden servir a los clientes con más rapidez. Pero los clientes desean garantías de que sus datos personales están seguros en los dispositivos. En la manufactura, hay un aumento en la cantidad de tecnologías portátiles que considerar. Este cambio significa asegurar el flujo de datos de un gran número de puntos finales.

Las metodologías de las aplicaciones también varían dependiendo del caso de uso y el tipo de dispositivo. Desde aplicaciones basadas en web, aplicaciones móviles nativas o aplicaciones híbridas, cada instancia impone exigencias de seguridad únicas en la empresa.

Las opciones disponibles de implementación móvil pueden añadir otro nivel de complejidad. Si la empresa incita a Traer Su Propio Dispositivo (Bring Your Own Device - BYOD) o utiliza la tecnología de nivel consumidor, el equipo de TI tendrá que comprometer recursos adicionales. Ellos tendrán que desarrollar soluciones de seguridad internas cuando los sistemas operativos móviles de nivel consumidor no proporcionan los niveles de seguridad necesarios. También hay preocupaciones adicionales cuando se trata de proteger la actividad de la red y la conectividad segura de WAN o WLAN.

Las plataformas de movilidad deben afrontar cada una de estas consideraciones mientras que responden a la demanda de tener más TI. Preservar la seguridad de los datos sin interrumpir las operaciones cotidianas debe ser el objetivo de cualquier empresa. ¿Cuáles son las amenazas principales y que debe incluir una póliza de seguridad móvil robusta?

HAY UN AUMENTO EN TECNOLOGÍAS PORTÁTILES QUE CONSIDERAR.

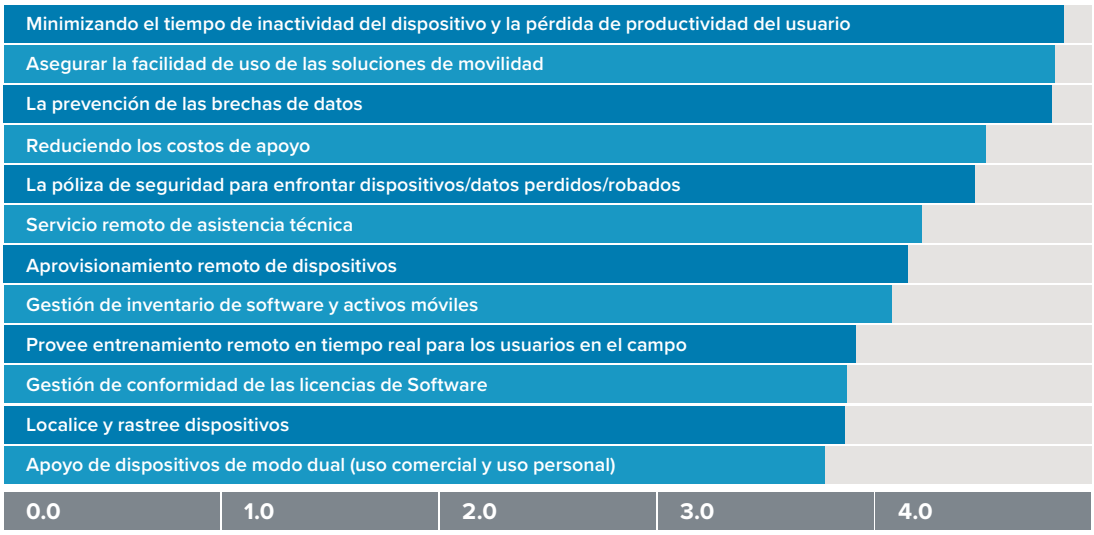
Este cambio significa asegurar el flujo de datos de un gran número de puntos finales.

Identificando los riesgos

En comparación con las computadoras de escritorio, los dispositivos móviles son más vulnerables a un alto número de amenazas de seguridad. El riesgo de robo es más alto debido al tamaño y la portabilidad de los dispositivos móviles. Los delincuentes cibernéticos se pueden aprovechar de las aplicaciones y los sistemas operativos si no son administrados adecuadamente. Además, la comunicación a través de conexiones celulares y Wi-Fi sin protección reduce la seguridad de los datos de la empresa o del cliente, lo que requiere consideración adicional para el control de acceso a redes no seguras.

De acuerdo a los analistas de VDC, la prevención de las brechas de datos es una de las cinco preocupaciones principales para las inversiones empresariales de movilidad. Las otras preocupaciones incluyen: minimizando el tiempo de inactividad, garantizando la facilidad de uso, la reducción de costos de apoyo y tener pólizas de seguridad establecidas para enfrontar los dispositivos y datos perdidos o robados. [1]

Evalué los siguientes problemas de movilidad en términos de importancia para su empresa
(1=extremadamente insignificante; 6=extremadamente importante)



[1] "Total Cost of Ownership Models - Enterprise and Government Mobility Applications", VDC Research, Josh Martin, David Krebs

Estos riesgos no son sencillos. Si averigua sobre los problemas generales de seguridad, encontrará amenazas tanto internas como externas. La investigación de VDC está corroborada por una encuesta de TechTarget SearchSecurity entre los cinco problemas más mencionados de la seguridad móvil empresarial.[1] Cada uno de los grandes problemas identificados por sus 487 encuestados se relacionan con las preocupaciones sobre los datos corporativos.

1. Pérdida de dispositivo – e.g. olvidando una tableta o un teléfono inteligente corporativo en un taxi o restaurante
2. Seguridad de aplicaciones – e.g. facilitando la disponibilidad de los datos a los desarrolladores de aplicaciones móviles gratuitas
3. Perdida de datos del dispositivo – e.g. el riesgo que los delincuentes cibernéticos accedan las aplicaciones corporativas que se ejecutan en dispositivos personales
4. Los ataques de malware – e.g. Troyanos, herramientas de supervisión o aplicaciones maliciosas
5. Robo de dispositivo – e.g. los datos expuestos después de que un dispositivo de superior calidad sea robado

Lo que está en cuestión es la reputación y los ingresos de la organización. De acuerdo a un artículo en CIO.com,[2] "Cuanto más los trabajadores y los contratistas utilizan dispositivos móviles para acceder los sistemas organizativos, aplicaciones y datos, más importante es proteger dicho acceso. Además, es esencial prevenir el acceso no autorizado a la información y a otros activos en los dispositivos supuestos a aumentar la productividad y el resultado final. La falta de prevención convierte los dispositivos en un peligro y posiblemente en una pérdida de ingresos."

La pregunta sigue siendo: ¿Qué medidas puede tomar su organización para enfrentar las amenazas de los problemas de seguridad móviles empresariales?

[1] Top 5 enterprise mobile security issues, Tech Target, 2012

[2] http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html

Combatiendo la amenaza

Con una dependencia creciente en tecnologías móviles, las empresas deben buscar una mejor respuesta a los problemas de seguridad. Una agregación de análisis de Gartner, Forrester e Information Week indica sólo algunas de las respuestas claves que los equipos de IT pueden tomar para enfrentar los riesgos internos y externos.

Forrester también recomienda usar las siete siguientes respuestas para la gestión de los dispositivos móviles (MDM):

- Aplicación de PIN (contraseñas seguras)
- Eliminación selectiva (esencial para un programa BYOD)
- Jailbreak / detección de root
- Cifrado de datos
- Redes virtuales privadas (VPN)
- Protección contra la pérdida de datos (evitando que los usuarios autorizados filtren datos por descuido o intencionalmente)
- Restricción del dispositivo ActiveSync

Si la empresa no está dispuesta a tomar en serio la seguridad móvil, las medidas realmente son una lista de deseos de TI. Los ejecutivos son clave en la elevación de seguridad a la sala de juntas y en comprometer recursos para combatir las amenazas cada vez más sofisticadas.

Para ser efectivo, vale la pena entender los requerimientos regulatorios comunes y las mejores prácticas internacionales de la seguridad. Una breve revisión de estas normas destaca las medidas que cada empresa debe incluir en su póliza de seguridad móvil:

- La protección contra dispositivos perdidos o robados
- La protección de datos en movimiento
- La protección de datos en reposo
- Mobile Application Management (gestión de aplicaciones móviles)
- Asegurando el cumplimiento de las regulaciones
- El control, administración y supervisión de dispositivos
- Protección de la privacidad de datos a alto nivel
- Minimizando los costos de administración para mantener las plataformas seguras
- Proporcionar fuertes autenticaciones/controles de acceso
- Maximizar el uso de la infraestructura de legado TI

Entonces, la empresa debe seguir adelante con una póliza móvil que incluye estas medidas de seguridad en su núcleo. Junto a los escenarios de caso de uso, la seguridad tendría que ser tan influyente en la selección de dispositivos y sistemas operativos.

CARACTERÍSTICAS DE GESTIÓN DE SEGURIDAD[3]
La inscripción automática y suministro de dispositivos
Contraseña forzada
Eliminación de datos y bloqueo remoto del dispositivo
Capacidad de auditoria de aplicaciones y de la cuenta del usuario
Detección de Jailbreak
Funciones de protección de datos
Controles de aplicación
NAC móvil
AV, anti -spam, FW punto final y el punto final IDS
Certificados basados en dispositivos
La supervisión activa de las protecciones anteriores
VPN corporativa
Gestión de claves, gestión de certificados

[3]Fuentes: informe de Information Week, noviembre de 2011; informe de Forester, Respuestas a preguntas más frecuentes de seguridad móvil, 2011; informe de Gartner, MCM_MQ abril de 2011.

El costo de tomar decisiones de movilidad

Dado a la proliferación de los riesgos de seguridad, las empresas deben evaluar el uso de dispositivos de nivel consumidor disponibles al momento. La mayoría de los dispositivos de nivel consumidor no vienen equipados con sistemas operativos conteniendo los requisitos de seguridad necesarios para las empresas. Los estudios demuestran que el costo total de propiedad (TCO) de dispositivos a nivel consumidor que utilizan aplicaciones empresariales puede ser entre el 40% y el 78% más alto que con los dispositivos diseñados para uso empresarial.[3] La seguridad es un elemento importante en este diferencial.

"Para el año 2016, 277 millones de dispositivos móviles utilizaran algún tipo de protección."

A menudo, los dispositivos de nivel consumidor utilizados en aplicaciones empresariales, son una invitación a una brecha de seguridad. En un estudio sobre BYOD hecho por Decisive Analytics[4], casi la mitad (46,5%) de las empresas encuestadas informaron una brecha de datos o de seguridad como resultado del uso de un dispositivo de nivel consumidor en la red empresarial. Inversiones importantes se están haciendo para contrarrestar esta amenaza. Sin embargo, no hay garantías de que estas soluciones de seguridad seguirán siendo eficaz contra las amenazas emergentes.

Por el contrario, los dispositivos robustos construidos para uso empresarial están diseñados para satisfacer y simplificar el cumplimiento con los mandatos claves de las regulaciones de seguridad. El alcance de cumplimiento de la seguridad puede variar, desde el muy amplio (e.g. entrenamiento del usuario) al muy detallado (e.g. validación de la integridad de los algoritmos criptográficos).

Ningún dispositivo o plataforma SO puede asegurar cumplimiento de forma independiente. Pero la obtención de dispositivos y plataformas de software a través de los fabricantes que se enfocan en los mandatos de seguridad, aumentará la probabilidad de cumplimiento y reducirá la carga administrativa de validación. Esto reduce el costo de las auditorías, puede evitar las multas/ sanciones monetarias, y puede eliminar la necesidad de reportar una brecha de datos - mejorando la ganancia neta.

[3] "Total Cost of Ownership Models - Enterprise and Government Mobility Applications", Josh Martin & David Krebs, VDC Research; "A 3 Year Cost Comparison of Consumer-grade vs. Durable Smart Devices", Jack Gold, Gold Associates

[4] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Enfoque sobre el sistema operativo y la seguridad de aplicaciones: Android

Las empresas considerando dispositivos de nivel consumidor tienen su selección de varias compañías importantes: Google, Apple y Microsoft. La plataforma Android de Google domina la cuota de mercado (81% del mercado global en 2015)[5]. La seguridad intrínseca los hace más atractivos a las empresas considerando modelos de nivel consumidor. Especialmente cuando se comparan con las plataformas SO móviles alternativas. El aislamiento de procesos, los permisos de accesos a recursos y la codificación de datos son algunos ejemplos de las características fuertes de seguridad de Android.

La mayoría de las preocupaciones con la seguridad de Android originan con el potencial de malware en GooglePlay – la tienda de aplicaciones de Android. Apple controla su tienda de aplicaciones porque mantienen control estricto sobre el proceso de firma digital. A pesar de esto, los riesgos de seguridad de GooglePlay se extienden a todas las tiendas de aplicaciones públicas. Todas son vulnerables a malware y a la invasión de privacidad (incluyendo el AppStore de Apple).

La mejor forma de implementar los dispositivos empresariales es proveer bloqueo de aplicaciones y/o utilizar una tienda de aplicaciones de confianza. Mobility Extensions (Mx) de Zebra ofrece mejor protección. Las empresas logran seguridad empresarial en los dispositivos de nivel consumidor a través de la simplificación del cumplimiento a los requisitos de movilidad y a las demandas regulatorias.

Para garantizar que los equipos de TI logren desplegar dispositivos de nivel consumidor con confianza, es necesario tener una tienda de aplicaciones empresariales, extensiones que incluyen listas blancas, autenticación AD/LDAP, gestión de claves y otras funciones de seguridad empresariales.

[5] http://www.idc.com/getdoc.jsp?containerId=prUS40664915

Está claro que la seguridad móvil es más que sólo asegurando la integridad de la empresa si hay una brecha de dispositivos o datos. Puede apoyar requisitos operacionales específicos a la estrategia móvil y reducir el costo total de propiedad a través de despliegues de movilidad empresariales. Principalmente, la seguridad móvil continuará evolucionando y requerirá vigilancia, revisión continua y actualizaciones.

Aunque la movilidad empresarial ha mejorado mucho en pocos años, la complejidad de seguridad ha cambiado y continuara cambiando. Los desafíos son complejos y las soluciones son amplias. Tendrán que ser explorados de forma individual y también tomando en cuenta las prioridades de la empresa. Es contraproducente tener una póliza de seguridad rigurosa si le restringe sus operaciones, causando que no sea competitivo y que sus trabajadores sean improductivos. Por otra parte, la falta de enfoco en la seguridad lo dejara vulnerable a los ataques. Las pólizas de seguridad móviles más robustas mitigaran los posibles riesgos, dejándolo libre para operar e innovar.

Es esencial balancear las prioridades en su póliza de seguridad móvil. Acomodando sus requisitos claves empresariales y las necesidades del usuario con pólizas de seguridad que coinciden con los diferentes casos de uso.

Una lista de control útil

Considerando la complejidad y las consideraciones claves, desarrollando la póliza de seguridad móvil empresarial aparece ser una tarea difícil. Esta lista de control lo ayudará asegurarse de que cualquier decisión que tome será exitosa para su empresa. Especialmente en el balanceo de los usuarios, la empresa y los requisitos de seguridad.

1 **Educar a todos:**
Asegúrese que todos estén consientes a las amenazas de seguridad y crear una póliza que detalle lo que se espera del usuario.

2 **Cambie las contraseñas frecuentemente:**
Cambie la contraseña por lo menos cada 30 días y considere obligar los cambios de contraseña (con criterios de seguridad) en sus aplicaciones.

3 **Obtenga una visibilidad completa de todos sus dispositivos:**
Utilice las herramientas de gestión de los dispositivos móviles para localizar dispositivos perdidos o robados inmediatamente y bloquee o borre los datos del dispositivo. Monitoree y utilice alertas para localizar cada dispositivo y saber cómo se está utilizando.

4 **Crear una lista blanca:**
Asegure que los usuarios puedan acceder sólo las páginas de web autorizadas, las que sean aprobadas para el uso con sus dispositivos.

5 **Protección contra malware:**
Puede proteger contra los vectores de infección con la implementación de una lista blanca para las aplicaciones internas y las fuentes de aplicaciones en sus dispositivos. Además, controlando la descarga de aplicaciones no autorizadas (sea de una conexión externa o por tarjeta de memoria) es una consideración clave para protegerse en contra de malware o aplicaciones nefarias.

6 **Actualización de sus dispositivos:**
Asegúrese que sus dispositivos estén al día con actualizaciones controladas y/o automáticas.

7 **Proteja sus datos:**
Configure sus dispositivos para guardar sus datos en áreas cifradas, protegiendo contra las brechas de datos.

8 **Despliegue de cifrado completo:**
Cuando se trabaja con datos sumamente confidenciales, puede cifrar los datos guardados en los dispositivos o los datos enviados por red inalámbrica.

9 **Utilice una tienda de aplicaciones empresarial:**
Debe evitar el acceso a las tiendas de aplicaciones públicas y solamente descargar las aplicaciones de una tienda empresarial de confianza.

10 **Reevalúe la seguridad constantemente:**
La seguridad móvil continúa evolucionando y requiere atención. Es importante actualizar las estrategias y prácticas para proteger contra las amenazas futuras.

VEA POR QUÉ LA SEGURIDAD ES SÓLO EL COMIENZO EN LA SELECCIÓN DE UN NUEVO SISTEMA OPERATIVO MÓVIL.

PARA EXPLORAR LAS OTRAS CONSIDERACIONES CLAVES, VISITE
WWW.ZEBRA.COM/MOBILITYREVOLUTION

ZEBRA

Sede NA y Corporativa
+1 800 423 0442
inquiry4@zebra.com

Sede Asia-Pacifíco
+65 6858 0722
contact.apac@zebra.com

Sede EMEA
zebra.com/locations
mseurope@zebra.com

Sede América Latina
+1 866 230 9494
la.contactme@zebra.com