ZEBRA

ESTABLECIMIENTO DE UNA SÓLIDA POLÍTICA DE SEGURIDAD MÓVIL: Principales riesgos y como pueden evitarlos las empresas.

La seguridad de la infraestructura de TI para movilidad empresarial suele compararse con los seguros. Algo que se justifica simplemente porque hay que tenerlo. Sin embargo, esta visión limitada se olvida de lo importante. La seguridad ofrece algo más que tan solo cobertura en respuesta a un evento concreto. También puede proporcionar garantía –al permitir que la empresa funcione e innove sin el riesgo de que se produzcan filtraciones de datos.

En este documento informativo, examinamos las principales consideraciones que hay que tener en cuenta para desarrollar una sólida política de seguridad móvil. Presentamos los principales riesgos y qué puede hacer para prevenirlos y poner en marcha nuevas oportunidades para mejorar la productividad, la eficiencia y la precisión en todas las operaciones.

No existe un único enfoque para todo

Hay algunas diferencias de opinión sobre la importancia de la seguridad. En lo que sí coincide todo el mundo es en que se trata de un asunto complejo que afecta a muchas áreas de la organización. Cuando se tiene en cuenta la diversidad de casos de uso de movilidad, las metodologías de aplicación y las opciones de despliegue de las distintas empresas, resulta más evidente la importancia global de la seguridad, así como su complejidad.

En un establecimiento de retail, el personal con tablets puede atender rápidamente a los clientes. Pero los clientes quieren garantías de que la información personal que proporcionan está segura en dichos dispositivos. En manufactura, hay que tener en cuenta el aumento de las tecnologías corporales. Este cambio supondrá proteger el flujo de datos de gran cantidad de terminales.

Las metodologías de aplicación también varían en función del caso de uso y el tipo de dispositivo. Desde aplicaciones basadas en la web hasta aplicaciones móviles nativas o incluso híbridas, cada caso plantea demandas de seguridad únicas en la empresa.

Las opciones de despliegue de dispositivos móviles disponibles pueden añadir otro nivel de complejidad. Si la empresa fomenta el uso del dispositivo propio (BYOD) o emplea tecnología de consumo, es posible que el equipo de TI tenga que asignar recursos adicionales. Tendrán que desarrollar soluciones de seguridad internas cuando los sistemas operativos para móviles de consumo no ofrezcan los niveles de seguridad necesarios. También existen otros problemas relacionados con la protección de la actividad de la red y la seguridad de la conectividad WAN o WLAN.

Las plataformas de movilidad deben enfrentarse a cada una de estas consideraciones de seguridad al tiempo que dan respuesta a la demanda incesante de la organización de más tecnologías de la información (TI). El objetivo de cualquier empresa debe ser proteger la seguridad de los datos sin interrumpir las operaciones diarias. Entonces, ¿cuáles son las principales amenazas y qué debe incluir una sólida política de seguridad móvil?

HAY QUE TENER EN CUENTA EL AUMENTO DE LAS TECNOLOGÍAS CORPORALES.

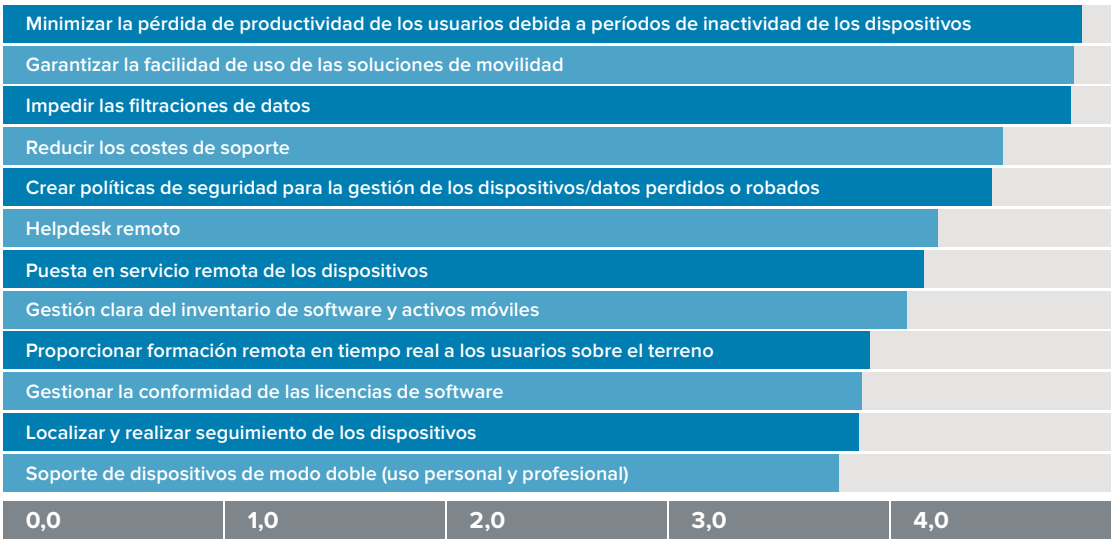
Este cambio supondrá proteger el flujo de datos de gran cantidad de terminales.

Identificación de los riesgos

Las características básicas de los dispositivos móviles implican que estos están expuestos a una cantidad mucho mayor de amenazas de seguridad en comparación con los dispositivos de escritorio. Debido a su factor de forma pequeño y portátil corren peligro de robo. Las aplicaciones y los sistemas operativos multiuso pueden abrir numerosas vías que los ciberdelincuentes pueden aprovechar si no se gestionan adecuadamente. Además, la comunicación por medio de conexiones Wi-Fi o móviles abiertas y desprotegidas reduce la protección de los datos del cliente o la empresa, con la consiguiente necesidad de dar mayor importancia al control del acceso a redes no protegidas.

Según los analistas de VDC, la necesidad de impedir las filtraciones de datos es una de las tres prioridades a la hora de invertir en movilidad empresarial. Disponer de políticas de seguridad para la gestión de dispositivos y datos perdidos o robados se encuentra también entre las cinco primeras prioridades –por detrás de minimizar los períodos de inactividad, garantizar la facilidad de uso y reducir los costes de soporte. [1]

Califique los siguientes problemas de movilidad en términos de su importancia para su empresa (1=muy poco importante; 6=muy importante)



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

No se trata tampoco de riesgos simples. Profundice en los problemas de seguridad dominantes y encontrará amenazas internas y externas. Una encuesta de TechTarget SearchSecurity sobre los cinco problemas más importantes de seguridad móvil en la empresa corrobora la investigación de VDC.[1] Cada uno de los grandes problemas identificados por los 487 encuestados están relacionados con su preocupación por los datos corporativos.

1. Pérdida de dispositivos – por ejemplo, dejarse un tablet o un smartphone de la empresa en un taxi o un restaurante
2. Seguridad de aplicaciones – por ejemplo, datos que se ponen a disposición de los desarrolladores de aplicaciones móviles gratuitas
3. Fuga de datos de dispositivos – por ejemplo, el riesgo de que ciberdelincuentes accedan a aplicaciones corporativas que se ejecutan en dispositivos personales
4. Ataques de malware – por ejemplo, troyanos, herramientas de supervisión o aplicaciones malintencionadas
5. Robo de dispositivos – por ejemplo, datos que quedan expuestos después de que se haya robado un dispositivo de categoría premium

Lo que está en juego son el prestigio y los ingresos de la organización. Como afirma un artículo en CIO.com,[2] *"Cuantos más empleados y contratistas usan dispositivos móviles para acceder a los sistemas, las aplicaciones y los datos de la organización, más importante es proteger esos accesos. Además, es esencial impedir que los dispositivos móviles, que se supone que aumentan la productividad e incrementan los beneficios, abran medios de acceso no autorizados a la información y otros activos; esto los convierte en un peligro y en una posible pérdida de ingresos".*

La pregunta sigue siendo: ¿Qué medida concreta puede tomar su organización para enfrentarse a la amenaza constante de los problemas de seguridad móvil en la empresa?

[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*

Cómo combatir la amenaza

Con una dependencia cada vez mayor de las tecnologías móviles, las empresas deben buscar una respuesta más fluida a los problemas de seguridad. Un conjunto de análisis realizados por Gartner, Forrester e Information Week muestra tan solo algunas de las respuestas que los equipos de TI pueden adoptar para prevenir los riesgos internos y externos.

Forrester recomienda además las siete respuestas siguientes como fundamentales para la gestión de dispositivos móviles (MDM) y la seguridad móvil:

- Aplicación de PIN (contraseñas seguras)
- Borrado selectivo de datos (esencial en el caso de un programa BYOD)
- Detección de jailbreak/root
- Cifrado de datos
- Redes privadas virtuales (VPN)
- Prevención de fuga de datos (impedir que usuarios no autorizados permitan la fuga de datos por descuido o malintencionadamente)
- Restricción de dispositivos ActiveSync

Ambos conjuntos de medidas solo son en la práctica "buenas intenciones" del departamento de TI si la empresa no está dispuesta a tomarse en serio la seguridad móvil. Los directivos desempeñan un papel fundamental para elevar la seguridad a la sala de juntas y comprometer recursos para combatir amenazas cada vez más sofisticadas.

Para conseguirlo, conviene entender los requisitos normativos más frecuentes y las prácticas internacionales recomendadas sobre seguridad. Un breve repaso a estos estándares pone de manifiesto las medidas que todas las empresas deben incluir en su política de seguridad móvil:

- Protegerse contra la pérdida o el robo de dispositivos
- Proteger los datos en movimiento
- Proteger los datos en reposo
- Gestión de aplicaciones móviles
- Garantizar el cumplimiento normativo
- Control, administración y supervisión de dispositivos
- Protección de la privacidad de datos de alto nivel
- Minimizar los costes administrativos para mantener plataformas seguras
- Proporcionar autenticación sólida/controles de acceso
- Maximizar el uso de la infraestructura de TI antigua

La empresa debe avanzar luego con una política de móviles que incluya como base estas medidas de seguridad. La seguridad debe tener la misma influencia que los casos de uso a la hora de elegir los dispositivos y el sistema operativo.

FUNCIONES DE GESTIÓN DE LA SEGURIDAD[3]
Inscripción automática y puesta en servicio de dispositivos
Contraseña obligada
Bloqueo remoto y borrado de datos de dispositivos
Funcionalidad de auditoría de cuentas de usuario y aplicaciones
Detección de jailbreak
Funciones de protección de datos
Controles de aplicaciones
NAC móvil
Antivirus, antispam, FW de terminales e IDS de terminales
Certificados basados en dispositivos
Supervisión activa de las protecciones anteriores
VPN corporativa
Gestión de certificados con gestión de claves

[3]*Fuentes: Informe de Information Week, noviembre de 2011; informe de Forester, Answers to top mobile security questions, 2011; informe de Gartner, MCM MQ, abril de 2011.*

El precio de tomar las decisiones de movilidad equivocadas

"277 millones de dispositivos móviles utilizarán algún tipo de protección en 2016".

Dada la proliferación de riesgos de seguridad, las empresas que se sienten atraídas por precios bajos deben reconsiderar el uso de dispositivos de consumo listos para usar. La mayoría de los sistemas operativos de consumo presentes en estos dispositivos no incluyen todas las funciones de seguridad que las empresas requieren. Hay estudios que muestran que el coste total de propiedad (TCO) de usar dispositivos de consumo para aplicaciones empresariales puede ser entre un 40% y un 78% más alto que el de los dispositivos empresariales creados ex profeso.[3] La seguridad es un elemento importante en esta diferencia de costes.

Los dispositivos de consumo empleados en aplicaciones empresariales suelen ser una invitación a una infracción de seguridad. En un estudio sobre BYOD realizado por Decisive Analytics[4], prácticamente la mitad (46,5%) de las empresas encuestadas comunicaron alguna filtración de datos o infracción de seguridad como consecuencia del acceso a la red corporativa de un dispositivo propiedad de un empleado. Se están haciendo importantes inversiones para contrarrestar esta amenaza. Sin embargo, no existe ninguna garantía de que estas soluciones a los problemas de seguridad sigan siendo eficaces ante amenazas emergentes.

Por el contrario, los dispositivos empresariales reforzados creados ex profeso se han diseñado y mejorado para satisfacer y simplificar el cumplimiento con importantes exigencias legales sobre seguridad. El ámbito de cumplimiento normativo sobre seguridad puede abarcar desde lo más general (por ejemplo, la formación de los usuarios) a lo más específico (por ejemplo, la validación de la integridad de los algoritmos criptográficos).

Ningún dispositivo ni plataforma de SO puede por sí solo garantizar el cumplimiento normativo. Pero si los dispositivos y las plataformas de software se adquieren de un fabricante centrado en las normas sobre seguridad aumentará la probabilidad de cumplimiento normativo y se reducirá la carga administrativa de validación. A su vez, esto reduce el coste en auditorías, puede evitar sanciones económicas y puede eliminar la necesidad de notificar una filtración de datos. Todo ello contribuye a aumentar los beneficios.

[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

La seguridad de las aplicaciones y el sistema operativo en el punto de mira: Android

Las empresas que buscan dispositivos de consumo tienen varios actores importantes del mercado entre los que elegir: Google, Apple y Microsoft. La plataforma Android de Google tiene la cuota dominante del mercado (81% del mercado global en 2015)[5]. Su oferta de seguridad intrínseca también la hace atractiva para las empresas que contemplen la posibilidad de adquirir dispositivos de consumo, sobre todo en comparación con las plataformas de SO para móviles de consumo alternativas. Espacio seguro para aplicaciones, permisos de acceso a recursos y cifrado de datos son tan solo algunos ejemplos de las funciones de seguridad reforzada de Android.

La mayoría de los problemas de seguridad de Android se originan en el malware potencial en GooglePlay –la tienda de aplicaciones de la plataforma. Apple protege firmemente sus aplicaciones de AppStore porque conserva un control estricto sobre el proceso de firma. A pesar de esto, el riesgo de seguridad con GooglePlay es extensivo a todas las tiendas de aplicaciones públicas. Todas son vulnerables a la invasión de la privacidad y al malware (incluso AppStore de Apple).

La práctica recomendada para ejecutar 'dispositivos con responsabilidad corporativa' es ofrecer bloqueo de aplicaciones y/o usar una tienda de aplicaciones empresariales de confianza. Mobility Extensions (Mx) de Zebra ofrece mayor protección. Si simplifican el cumplimiento normativo de las exigencias legales y los requisitos de movilidad, las empresas pueden disfrutar de seguridad de categoría empresarial en dispositivos de consumo.

En combinación con una tienda de aplicaciones empresariales, extensiones como listas blancas, autenticación LDAP/AD, gestión de claves y otra funcionalidad básica de seguridad empresarial garantizan que los equipos de TI puedan distribuir dispositivos de consumo con toda confianza.

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

Lo que es evidente es que la seguridad móvil es mucho más que garantizar la integridad de la empresa en caso de filtración de datos e infracción de dispositivos. Puede admitir requisitos operativos específicos para la estrategia de movilidad global y reducir el coste total de propiedad en todas las implementaciones de movilidad empresarial. Lo más importante es que la seguridad móvil seguirá evolucionando y necesitará revisiones y actualizaciones atentas y constantes.

Aunque la movilidad empresarial ha recorrido un largo camino en apenas unos años, la complejidad del panorama de la seguridad ha cambiado (y sigue haciéndolo) hasta resultar irreconocible. Los retos son complejos y las soluciones numerosas. Deben examinarse individualmente y en conjunto con las prioridades de la organización. Es inútil tener una política de seguridad estricta si limita las operaciones y ello le impide ser competitivo y reduce la productividad de sus trabajadores. Por otra parte, si se centra en todo menos en la seguridad quedará expuesto a ataques. Las políticas de seguridad móvil más sólidas mitigarán los riesgos a los que se enfrenta y le permitirán funcionar e innovar.

La clave es equilibrar las prioridades contenidas en la política de seguridad móvil –incorpore los principales requisitos de su empresa y las necesidades de los usuarios finales a políticas de seguridad subordinadas que se ajusten a distintos casos de uso.

Una práctica lista de comprobación

Dada la complejidad y el número de consideraciones importantes, el desarrollo de una política de seguridad móvil para el personal puede parecer una tarea difícil. Esta lista de comprobación debe ayudarle a asegurarse de que lo que elija funciona bien en toda la organización –sobre todo en lo que respecta a equilibrar los requisitos del usuario, de la empresa y de la seguridad.

1. **Concienciar a todo el mundo:**
Asegúrese de que todos estén al tanto de las amenazas de seguridad y cree políticas de uso claras que expliquen lo que se pretende.

2. **Cambiar de contraseña periódicamente:**
La práctica recomendada es actualizar las contraseñas cada 30 días como mínimo, además, debe plantearse la posibilidad de incorporar cambios de contraseña obligatorios (con criterios de seguridad de la contraseña) en las aplicaciones.

3. **Tener visibilidad completa de todos los dispositivos:**
Use herramientas de gestión de dispositivos móviles para localizar inmediatamente los dispositivos perdidos o robados y eliminar el dispositivo o borrar los datos. Use además supervisión y alertas para saber dónde está cada dispositivo y cómo se usa.

4. **Crear una lista blanca:**
Asegure el acceso de los empleados únicamente a una lista blanca de sitios web –cuyo uso autorice en sus dispositivos.

5. **Protegerse contra el malware:**
Si incluye listas blancas de las aplicaciones internas y los orígenes de aplicaciones en los dispositivos, puede protegerse contra vectores de infección. Asimismo, al controlar la posibilidad de que los dispositivos 'transfieran localmente' aplicaciones externas –tanto por medio de una conexión externa como de una tarjeta de almacenamiento– es crucial que se proteja contra el malware y otras aplicaciones malintencionadas.

6. **Actualizar los dispositivos:**
Asegúrese de que los dispositivos ejecutan siempre el software más reciente, con actualizaciones controladas y/o automáticas.

7. **Incluir los datos en contenedores:**
Configure los dispositivos de tal forma que los datos se incluyan en contenedores en distintas áreas cifradas, lo que hace prácticamente imposible que los atacantes accedan a los datos.

8. **Desplegar cifrado completo:**
Cuando los empleados trabajen con datos estrictamente confidenciales, puede cifrar los datos almacenados en los dispositivos, así como los datos enviados por redes inalámbricas.

9. **Usar una tienda de aplicaciones empresariales:**
Debe evitarse el acceso a tiendas de aplicaciones públicas y las aplicaciones deben descargarse de una tienda de aplicaciones empresariales de confianza.

10. **Reconsiderar continuamente la seguridad:**
La seguridad móvil no es algo que se establece y después podemos olvidarnos de ella, sino que es fundamental actualizar continuamente las estrategias y prácticas recomendadas para gestionar las amenazas en constante evolución.

VEA POR QUÉ LA SEGURIDAD ES TAN SOLO EL COMIENZO CUANDO SE ELIGE UN NUEVO SO PARA MÓVILES.

EXAMINE LAS DEMÁS CONSIDERACIONES IMPORTANTES EN WWW.ZEBRA.COM/MOBILITYREVOLUTION

ZEBRA

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

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

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

Sede en Latinoamérica
+1 847 955 2283
la.contactme@zebra.com