THE STANDARD
INSIDE
Edición patrocinada por Symantec.

Edición Febrero 2015.
Año 1. Número 1.

The Standard Inside es una publicación de The HAP Group, casa editora de CIO América Latina y PC World En Español.

Los cibercriminales van por los móviles

6 maneras diferentes de perder sus datos móviles...
Y ni siquiera darse cuenta

La seguridad móvil es posible con Symantec Mobility: Suite

Conozca cómo proteger sus datos

Los cibercriminales van por los móviles

Los dispositivos móviles son el nuevo gran objetivo para los ciberdelincuentes que buscan hacer dinero rápido. Según el Reporte de Norton, 38% de los usuarios de teléfonos inteligentes ya han sido víctima de la delincuencia cibernética.

En el pasado los cibercriminales perseguían la fama. Hoy están a la caza de ganancias millonarias. Y así como la gente prefiere a los teléfonos inteligentes y las tabletas como dispositivos de computación primaria, en detrimento de las computadoras personales, también los estafadores digi–tales aplican todas sus des–trezas y conocimientos para sacar ventajas de la ingenuidad y descuido de los usuarios.

Los móviles son el nuevo gran objetivo para los ciberdelincuentes que buscan hacer dinero rápido. Según el **Reporte 2013 de Norton**, 38% de los usuarios de teléfonos inteligentes ya han sido víctima de la delincuencia cibernética.

Descargue el Reporte Norton

No es por ninguna coincidencia que el aumento de las amenazas a dispositivos móviles coincida con la adopción y el uso de un mercado abierto generalizado de Android. Los usuarios de Android representan el mayor mercado potencial para los ciberdelincuentes. ¿La razón? Las aplicaciones que se ofrecen a través de los mercados de terceros, que proporcionan una manera fácil para robar al dueño del dispositivo.

¿Cuánto dinero están haciendo los cibercriminales con los móviles? Eso varía ya que la mayoría de los ataques depende principalmente de la cantidad de usuarios que descarguen e instalen aplicaciones maliciosas.

Hemos visto casos en los que las previsiones de ingresos podría potencialmente llegar a millones de dólares .La piratería informática móvil es un negocio muy lucrativo para los proveedores de aplicaciones de malware.

Una de las piezas de malware más poderosas y costosas de que se consigue en mercado negro es IBanking , que los desarrolladores están ofreciendo por 5,000 USD la suscripción.

En las próximas líneas conozca cómo los estafadores están monetizando sus ataques a móviles.

Fraude en las tarifas de facturación

En este escenario, los atacantes configuran y registran un número de tarificación adicional en los servicios de telefonía. Por lo general, utilizan "códigos de acceso" que son más cortos que un número de teléfono normal, y agregan con una prima superior al costo normal de una llamada de SMS.

¿Y cómo opera? El atacante configura una aplicación maliciosa y la libera en el mercado de las aplicaciones. Después un usuario incauto se descarga la aplicación en su dispositivo, la aplicación enviará periódicamente mensajes SMS al número de tarificación adicional.

Dado que la aplicación puede solicitar de forma encubierta permisos para enviar mensajes durante la instalación, ésta puede vulnerar datos y enviarlos al atacante a través de mensajes sin confirmación del usuario. Al mismo tiempo, el propietario del teléfono incurre cargos en su factura de teléfono y el hacker cobra cantidades que varían entre los 10 hasta 50 USD.

Estafas en aplicaciones

Las estafas móviles por lo general vienen en forma de aplicaciones inútiles o engañosas, que solicitan pagos sin necesidad de firmar con el usuario el servicio prestado.

Hemos visto aplicaciones de fraude de un solo clic en Japón que los estafadores usan a través del pago de una cuota por el uso de los sitios relacionados con adultos. El usuario utiliza varios enlaces a sitios de videos con contenido para adultos, y el estafador mezcla sus enlaces maliciosos entre los enlaces legítimos que ataca al reproducir un vídeo.

Madware

Los desarrolladores pueden monetizar aplicaciones móviles mediante la visualización de anuncios. Muchas redes de publicidad pagan a los pro–veedores de contenido por cada visita y cuando se muestran sus anuncios.

Por desgracia, los ciberdelincuentes están aprovechando este modelo de negocio usan–do aplicaciones maliciosas con las bibliotecas de anuncios agresivos, llamado madware.

Recientemente, hemos visto un nuevo grupo de aplicaciones maliciosas, apodado Android.Simplocker, que toman los archivos almacenados en los dispositivos móviles como rehenes por la encriptación de ellos. Una vez que la aplicación se descarga, el malware muestra un mensaje en pantalla que indica que el teléfono ha sido bloqueado. Con el fin de desbloquear el dispositivo de la aplicación el hacker establece un pago que el usuario se verá obligado a cancelar.

El spyware

Existen múltiples aplicaciones de Android que permiten a alguien realizar un seguimiento y monitorear otros usuarios de teléfonos móviles. Por ejemplo, estas aplicaciones pueden grabar y exportar todos los mensajes, correos electrónicos, registros de llamadas, ubicaciones GPS SMS o activar el micrófono del teléfono.

Los ejemplos incluyen Android. Tapsnake y Spyware.Flexispy, que puede costar hasta 400 USD. Mientras que las aplicaciones como el software espía no pueden generar ingresos para el atacante, son una forma rápida para el pro–veedor de la aplicación espía para sacar provecho.

Intercepción de las transacciones móviles

Para los clientes que utilizan cuentas bancarias móviles en línea, muchos bancos utilizan mTANs, (números de autenticación de transacciones móviles), como un mecanismo de seguridad para evitar que los ciber-criminales comprometan las cuentas de banca en línea.

Aunque las tácticas anteriores representan la mayor parte de los esquemas existentes en el mercado de Android, todavía existen posibilidades de que aparezcan otras a futuro.

Las próximas oportunidades económicas para los ciber-delincuentes probablemente incluyan la adaptación de más ataques de PC en el entorno móvil. Esto puede significar la posibilidad de ataques más sofisticados dirigidos contra dispositivos móviles, así como el mejoramiento de las técnicas por parte de los cibercriminales.

¿Qué arriesgas al perder tu smartphone?

El Proyecto Honey Stick de Symantec es un experimento que se hizo en México con 30 smartphones que fueron dejados como "perdidos" en tres ciudades del país. Antes de que los teléfonos fuesen abandonados intencionalmente, se prepararon con aplicaciones e información personal y corporativa, además de habilitarles la capacidad de ser monitoreados para saber qué pasaba con los equipos cuando alguien los encontraba. Esta prueba se realizó también en los Estados Unidos y Canadá.

Entre los hallazgos destaca que, cuando alguien pierde su teléfono, existe una alta probabilidad de que quien lo encuentre tenga acceso a la información personal y de trabajo que está en el dispositivo, sobre todo si no se cuenta con la protección adecuada. Además, el dueño de un smartphone no debe asumir que quien lo encuentre le buscará para devolvérselo y debe saber que, aunque logre recuperar su dispositivo, no existe garantía de que no fue violada la privacidad sobre su información.

Resumen de accesos por aplicación

Aplicación accedida	Total Número de teléfonos/porcentaje
Contactos	20 (67%)
Fotos privadas	24 (80%)
Redes sociales	24 (80%)
Administrador Remoto	19 (63%)
Contraseñas	18 (60%)
Casos RH (PDF)	16 (53%)
Salarios RH (Hoja de cálculo)	15 (50%)
Webmail (Correo personal)	14 (47%)
Calendario	12 (40%)
Correo electrónico corporativo	12 (40%)
Documentos en la nube	11 (37%)
Banca en línea	11 (37%)
Accesos a través de una pantalla con credenciales predeterminadas (acceso intencional a información crítica)	23 (77%)
Intentos de regresar el *smartphone*	5 (17%)

6 maneras diferentes de perder sus datos móviles...Y ni siquiera darse cuenta

Compartimos los seis riesgos más comunes y le indicamos cómo reducirlos para proteger su información personal y de trabajo

Uno de los principales temores, o quizás el principal, en esta era de la informática y las comunicaciones por Internet es la de extraviar o perder los datos que uno guarda en su celular, tablet, laptop o cualquier otro dispositivo electrónico móvil.

En este sentido, Symantec ha identificado las seis principales amenazas que nos acechan en el mundo real y cómo combatirlas y lograr la seguridad que usted y su negocio requiere.

La movilidad

Hablemos de los dispositivos móviles de sus empleados. Sí, esos que les encanta usar en su tiempo libre o personal, se han convertido ahora en la principal herramienta de trabajo.

Una reciente investigación arroja los siguientes datos: el 65% de las empresas que fueron encuestadas, otorgan a sus empleados acceso a la red a través de sus propios recursos.

Por otra parte, el 80% de las aplicaciones que estos empleados usan no están basadas en las instalaciones, pero sí en la nube; y 52% utiliza regularmente, no uno, sino tres o más dispositivos.

Claro, estas aplicaciones uno las guarda en los teléfonos inteligentes, computadoras portátiles y tabletas, lo que abre nuevas oportunidades para la productividad móvil.

Pero es ahí, por su naturaleza, donde la movilidad se hace escanrio de mayores vulnerabilidades, que se traduce en nuevas maneras de perder datos, perder la protección y perder la confianza en la seguridad de la data empresarial. Afortunadamente la productividad y la protección pueden viajar juntas, si usted entiende completamente lo que los riesgos son y lo que se puede hacer para mitigarlos.

Este artículo revisa brevemente las seis principales amenazas a su fuerza de trabajo móvil, igualando los peligros del mundo real con formas realmente útiles y que pueden lograr la seguridad que su negocio requiere.

Pérdida y/o robo

1 El riesgo más obvio a menudo se une con la respuesta más obvia: anticiparse a la sustitución de los dispositivos perdidos. Sin embargo, muchos dispositivos de trabajo son propiedad de los propios empleados.

Pero más importante aún es lo que está en el dispositivo, no es el dispositivo en sí, lo que verdaderamente importa. Cada móvil perdido es un portal abierto a quienes desean conocer y robarse las aplicaciones y los datos de su empresa.

> ¿Dónde está su celular?

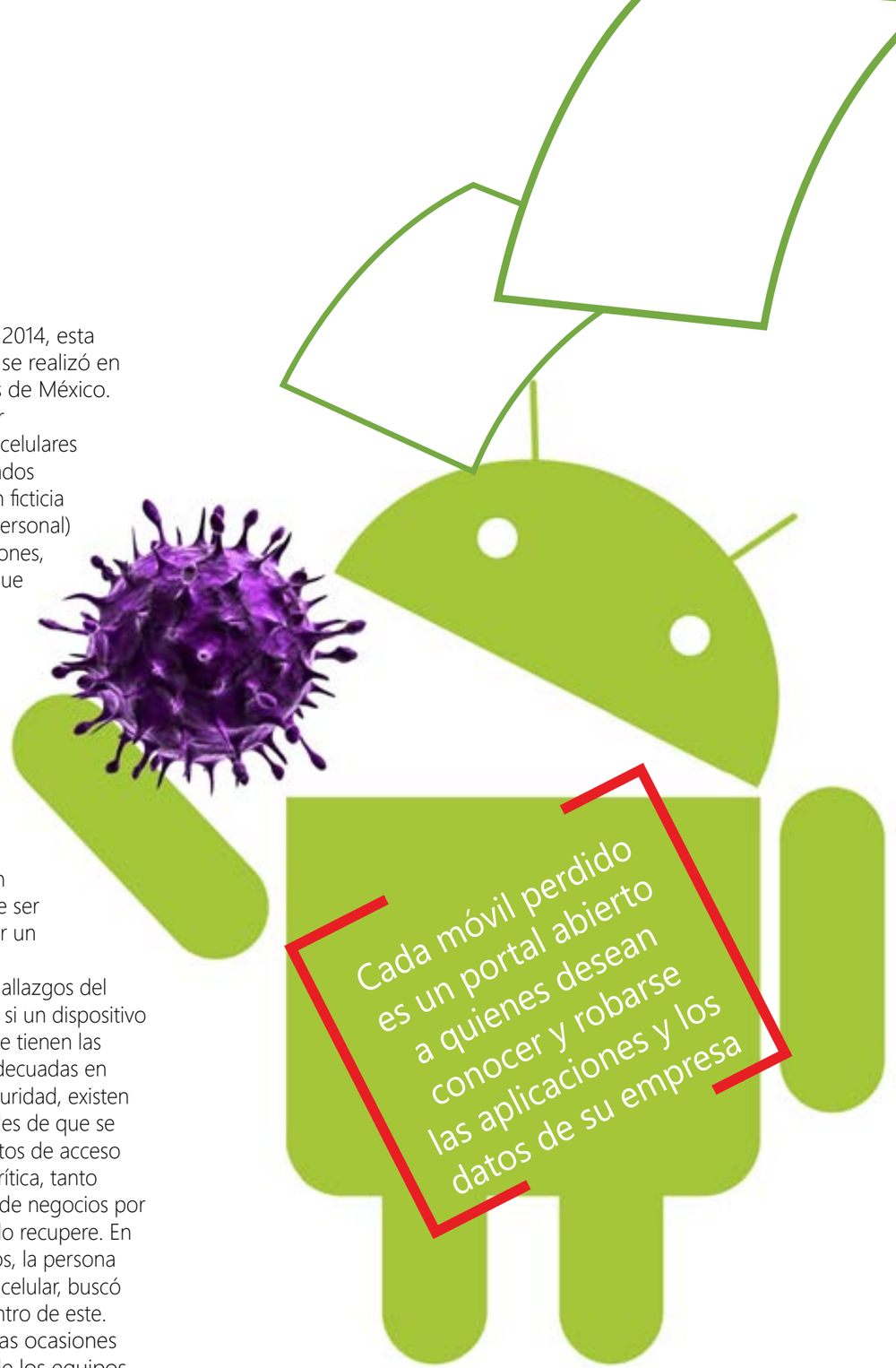
¿Se estará exagerando el problema? En 2012, Symantec puso nuestras preocupaciones a prueba. En una investigación denominada Proyecto Honey Stick, voluntariamente se extraviaron diez teléfonos inteligentes en cuatro ciudades de los Estados Unidos y en una

de Canadá. En 2014, esta comprobación se realizó en varias ciudades de México.

Antes de ser "olvidados", los celulares fueron precargados con información ficticia (corporativa y personal) y varias aplicaciones, para asegurar que los dispositivos parecieran normales. Además, se habilitó la capacidad de ser monito–reados de manera remota para conocer lo que sucedía con ellos después de ser recuperados por un desconocido.

Uno de los hallazgos del estudio fue que si un dispositivo se pierde y no se tienen las precauciones adecuadas en cuanto a su seguridad, existen altas posibilidades de que se presenten intentos de acceso a información crítica, tanto personal como de negocios por parte de quien lo recupere. En 97% de los casos, la persona que se hizo del celular, buscó información dentro de este.

En 87% de las ocasiones de utilización de los equipos, el objetivo fue ingresar en aplicaciones o datos corporativos y en el 90% de los intentos para entrar en aplicaciones o información personal.



La persona que pierde un teléfono móvil en México no debe esperar que quien lo encuentre se comunique para devolverlo. Solo en el 17% de los casos (5 de 30 equipos), hubo algún intento de regresarlo. Además, aun siendo contactado, el propietario no debe asumir que su información esté intacta.

¿Cuál es la lección? En lugar de centrarse en los dispositivos perdidos, las empresas necesitan proteger los datos sensibles que podrían potencialmente extraviarse y que forman parte de cualquier equipo básico.

Esta gestión debe complementarse con políticas de aplicación y protección de datos. En un nivel gerencial, esto significa que debe existir una función que tenga la capacidad de localizar rápidamente los dispositivos perdidos.

Para la protección a un nivel más profundo, las empresas deben asegurar las aplicaciones y cifrar los datos corporativos.

2 Fuga de datos

Mucho se ha dicho acerca de las amenazas de los "insiders" malévolos que deliberadamente buscan y comparten la información comercial confidencial.

Pero la mayor amenaza puede ser la de empleados benévolos y bien intencionados, que utilizan los servicios basados en la nube, como el correo electrónico y herramientas de colaboración en línea, para conseguir simplemente más trabajo con mayor rapidez.

En un camino de constante evolución hacia una mayor facilidad de uso (también conocido como "consumerización"), los empleados se sienten cómodos trabajando con aplicaciones diseñadas para el beneficio de los consumidores, no por las preocupaciones de seguridad de las corporaciones.

Pero una vez en la nube, los datos de la empresa puede estar más allá de su control. Los programas de intercambio de archivos y edición de documentos son populares entre los empleados, y por lo general carecen de los protocolos de acceso y autorización que necesitan las empresas para la protección de datos. Sin controles deliberados, los datos pueden "fugarse" hacia otros destinos, no tan plácidos o conocidos de la esfera de TI corporativa y "caer" en el mundo menos seguro de los riesgos.

Una aplicación apropiada para la protección de datos debe adoptar un enfoque de dos vías para la seguridad: 1) la aplicación de una lista negra de aplicaciones que prohíbe el acceso a aplicaciones no autorizadas; y 2) la implementación de controles que previenen los datos de negocio de ser copiado, pegado y / o de cualquier otra manera compartida a través de las aplicaciones en línea.

Las capacidades de aplicaciones y protección de datos relevantes incluyen:

- Autenticación de cada App específica.
- El cifrado de datos.
- Copiar / pegar bloqueo.
- Desactivación de uso compartido de documentos.
- El bloqueo de acceso a los dispositivos modificados.

3 Los ataques de malware y maliciosos

En números concretos, muchos ataques de malware amenazan más a los PCs que los dispositivos móviles. Pero las cantidades de los ataques a los dispositivos móviles está creciendo y de manera muy rápida.

Mientras que los profesionales de TI tradicionales no le están prestando mucha atención a los

> Los profesionales de TI tradicionales no le están prestando mucha atención a los malware en móviles

malware para móviles, los malos ven como su móvil está para ser robado, hackeado o interceptado.

Entre las mayores amenazas está el robo de identidad, la exposición de la información y la pérdida de datos efectuados por ataques maliciosos de los caballos de Troya, monitores y el malware autoestopistas.

De éstos, la mayor amenaza puede ser los apps "falsificados"; bajo el camuflaje de un juego o una aplicación popular. El atractivo de libre descarga hace que estas aplicaciones puedan colarse con un código malicioso en el dispositivo, que puede rozar el dinero de las cuentas o extraer datos de las redes de negocios.

El llamado freeware de "seguridad" carece de la suficiente fuerza e inteligencia para hacer frente a la constantemente mutación de diversos malware. La verddera protección eficaz contra cualquier amenaza debe dar cuenta de las variaciones en el perfil de riesgo entre diferentes plataformas, y aplicar una acción coordinada para asegurar los activos empresariales.

4 Los dispositivos compartidos y contraseñas

Según estudios recientes, cerca de la mitad de todos los empleados comparten sus dispositivos con los amigos y la familia; otro 20% su cuota de su contraseñas. Por desgracia, el intercambio informal de cuentas representa a la mayoría de las violaciones de la seguridad personal.

La protección de los dispositivos móviles es mucho más que la aplicación de un ScreenLock. Para que los usuarios puedan acceder a los datos de negocio y aplicaciones, puede ser prudente autenticar sus identidades.

Considere la posibilidad de la aplicación de un enfoque de dos factores para la autenticación, es decir, la clave de usuario y una aplicación exitosa de gestión de acceso.

5 Jailbreaking y enraizamiento

En un mundo BYOD, es fácil para un empleado introducir un dispositivo "arraigado" o "cárcel-roto" en el entorno corporativo. Dicho dispositivo y sus modificaciones pueden eludir los protocolos de seguridad, las características de seguridad de desinstalación, y el acceso abierto a los sistemas de archivos previamente protegidas y a los datos y demás controles.

Las empresas necesitan aplicar políticas de gestión de dispositivos que se apliquen bajo normas coherentes para la configuración y la seguridad en todos los dispositivos, así sean propiedad de la empresa, o de los empleados.

6 Wi-Fi gratuita y espionaje inalámbrico

Si se trata de "libre", es probable que sea falso; cualquier hot spot que se llame visible en sí "libre", es probable que sea la pesca de datos en movimiento. Los usuarios a menudo no reconocen su vulnerabilidad, y las empresas no tienen control o visibilidad en canales 3G, 4G y 4G LTE.

Las aplicaciones, datos y políticas completas de gestión de dispositivos deben proteger a dos niveles:

- La comunicación, como el correo electrónico corporativo, a través de SSL segura o conexiones VPN.
- Cifrado de datos corporativo, cuando está en tránsito y en reposo dentro de los dispositivos móviles.

Symantec Mobility: Suite

Hoy en día tomar ventaja de la movilidad

y tener acceso seguro a los datos en cualquier momento y en cualquier lugar puede ser un diferenciador de negocio y acelerar la productividad. Así lo reconocen tanto empresas, como empleados.

Para el CIO, ofrecer acceso móvil a la información empresarial implica desafíos importantes como son la protección de los datos corporativos en los dispositivos, la separación de la información personal y corporativa, y la gestión de diversos sistemas operativos. Todos enmarcados en la prevención de los datos, los dispositivos y las aplicaciones para evitar que se conviertan en otro vector de ataques.

Las organizaciones pueden adoptar una solución unificada de control que les ayude a cumplir las normas de seguridad consistentemente, independiente del tipo de dispositivo y sin obstaculizar la productividad del usuario final o la privacidad.

Symantec Mobility Suite simplifica la gestión de la movilidad, la integración de la gestión de dispositivos móviles (MDM), gestión de aplicaciones móviles (MAM) y protección contra amenazas móviles, en un modelo integrado en una consola.

Si el entorno de un usua–rio ha sido estandarizado en los dispositivos de propiedad de las empresas, entonces les permite un programa de 'elegir su propio dispositivo' (CYOD), o "traiga su propio dispositivo" (BYOD) o administre una combinación de estas opciones. Mobility Suite hace que sea más fácil para las empresas dominar la seguridad, al tiempo que maximiza la productividad.

Esta solución para la gestión de móviles es la más novedosa en el mercado. A lo largo de los años Symantec ha adquirido e incorporado diversas tecnologías relacionadas con la movilidad de compañías como Nukona, Odisea y NitroDesk.

Mobility Suite integra estas adquisiciones en una solución que hace fácil para los clientes aplicar la movilidad con una solución completa y flexible que le da opciones de los clientes para la protección por capas.

En la oferta de esta solución, los clientes tienen la opción de adquirir la licencia de Symantec en conjunto de forma independiente con los módulos individuales: Movilidad; Admi–nistración de dispositivos (MDM), Administración de aplicaciones (MAM), o Protección contra amenazas. La solución ofrece soporte para Windows Phone 8.1, Samsung SAFE, y iOS 8.

Soporte para los proveedores de servicios

Proveer soluciones de gestión para la movilidad empresarial es una gran oportunidad de negocios para las empresas que brindan servicios. Symantec facilita el implementar y ofrecer cualquier servicio a los clientes. Con las capacidades de multitenencia y APIs de integración adicionales, los socios proveedores de servicios pueden fácilmente conectarse con Mobility Suite en su infraestructura para la gestión de los servicios.