MobileIron

INFORME SOBRE SEGURIDAD MÓVIL Y RIESGOS

TERCERA EDICIÓN

RESUMEN EJECUTIVO

Bienvenidos a la tercera edición del Informe sobre Seguridad Móvil y Riesgos de MobileIron. Este Informe bianual proporciona a los líderes en seguridad informática información puntual sobre el panorama general de amenazas móviles y los riesgos emergentes a los que se enfrentan sus organizaciones.

ESTA EDICIÓN INCLUYE:

DATOS REGIONALES

de Australia, Bélgica, Francia, Alemania, Japón, Países Bajos, España, Reino Unido y Estados Unidos

DATOS ESPECÍFICOS DEL SECTOR

datos para los servicios financieros, las administraciones y el sector sanitario

ESTADÍSTICAS

sobre la adopción del Programa de Inscripción de Dispositivos (DEP) y el Programa de Compras por Volumen (PCV) de Apple

Las aplicaciones corporativas

MÁS POPULARES

Las aplicaciones móviles

MÁS BLOQUEADAS

ÁREAS QUE EXPERIMENTARON LEVES CAMBIOS O MEJORAS DURANTE LOS ÚLTIMOS SEIS MESES:

29 %

de empresas tenía políticas desactualizadas

SÓLO EL 55 %

impusieron siempre políticas de seguridad

MENOS DEL 5 %

implementaron antimalware móvil

Para ayudar a las organizaciones tecnológicas a que incorporen la mitigación de riesgos como parte de su rutina de seguridad móvil, hemos desarrollado el Listado de Verificación de Prioridades de Ciberhigiene.

SITUACIÓN GENERAL DE LAS AMENAZAS MÓVILES

NUEVAS AMENAZAS Y TENDENCIAS

Casi inmediatamente después de haber publicado la segunda edición de este informe, comenzaron a aparecer vulnerabilidades importantes y nuevas líneas de malware. El malware Godless, identificado a finales de julio de 2016, logró infectar unos 850.000 dispositivos[1]. Inicialmente descubierto en febrero de 2016, Hummingbad se analizó con mayor profundidad en julio y, al parecer, fue creado por Yingmob, el grupo que está detrás del malware de iOs YiSpectre que acaparó los titulares el año pasado. Hummingbad logró infectar casi 85 millones de dispositivos[2]. El aparente objetivo de ambas líneas de malware era generar ingresos mediante publicidad fraudulenta. No obstante, lo que es más notable —y siniestro— es que contenían vulnerabilidades que intentaban descifrar dispositivos de forma inalámbrica sin que el usuario lo supiera, otorgando de este modo a los atacantes un control total sobre el dispositivo infectado.

«HUMMINGBAD LOGRÓ INFECTAR A CASI 85 MILLONES DE DISPOSITIVOS»

Ese mismo verano, se identificó una serie de cuatro vulnerabilidades denominadas «QuadRooter» en el firmware de Android para los conjuntos de chips de banda base Qualcomm. Estas vulnerabilidades afectaron aproximadamente a 900 millones de dispositivos, pero se mitigaron en gran medida gracias a la función Verify Apps de Google Play y Android[3].

Las vulnerabilidades y el malware más destacados y peligrosos de iOS hasta la fecha han sido Trident/Pegasus, una serie de tres vulnerabilidades que fue necesario explotar conjuntamente[4]. Al igual que Godless y Hummingbad, las vulnerabilidades Trident ofrecían a los atacantes un método para hacer un «jailbreak» de forma inalámbrica en los dispositivos y, a continuación, instalar el spyware Pegasus, que era capaz de interceptar prácticamente todas las comunicaciones de entrada y salida del dispositivo.

Posteriormente, ese otoño, comenzaron a circular vulnerabilidades de la seguridad de Android para una clásica vulnerabilidad de Linux Kernel conocida como "Dirty COW" (CVE-2016-5195), que continuó una prolongada tendencia de vulnerabilidades de Open Source Software que afectaron a dispositivos y aplicaciones móviles[5]. Poco después, una línea de malware llamada Gooligan afectó a un millón de cuentas de usuarios de Google que utilizaban aplicaciones que se descargaban en app stores de terceros[6]. Al igual que otras líneas de malware, Gooligan «descifraba» dispositivos infectados y recopilaba tokens de autenticación que permitían a los atacantes acceder a los datos del usuario desde una gran variedad de servicios Google.

En último lugar, el agente Adups puso en riesgo los auriculares del fabricante BLU al transmitir registros de llamadas, mensajes SMS, información sobre localización y otros datos a servidores en China. Adups se posiciona como una herramienta de aprovisionamiento de firmware de Android, pero la Compatibility Test Suite (CTS) de Android la ha bloqueado.

[1] Identificado por Trend Micro, http://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices/

[2] Identificado por Check Point Software Technologies, http://blog.checkpoint.com/2016/07/01/from-hummingbad-to-worse-new-in-depth-details-and-analysis-of-the-hummingbad-andriod-malware-campaign/

[3] Identificado por Check Point Software Technologies, http://blog.checkpoint.com/2016/08/07/quadrooter/

[4] Identificado por Lookout and Citizen Lab, https://blog.lookout.com/blog/2016/08/25/trident-pegasus/

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195

[6] Identificado por Check Point Software Technologies, http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/

EL ESTADO DE LA SEGURIDAD CORPORATIVA MÓVIL

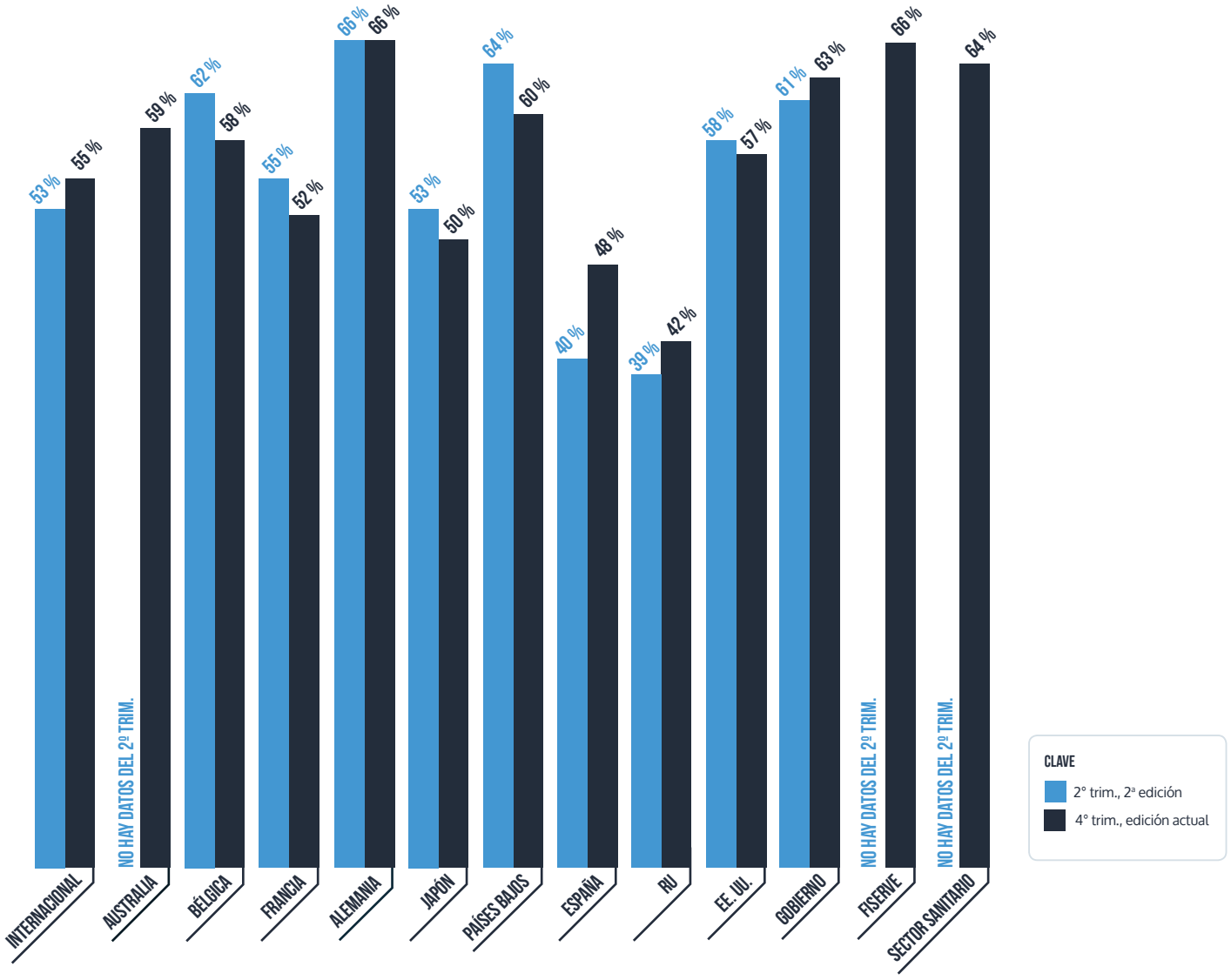
CUMPLIMIENTO DE POLÍTICAS

Las relaciones informáticas dedican tiempo y recursos a configurar políticas de seguridad móvil, pero no siempre imponen su cumplimiento. A finales de 2016, casi la mitad de las empresas no habían aplicado las políticas en los dispositivos, una cifra que se mantuvo el 2° trimestre. Alemania tuvo el porcentaje más alto de empresas que sí impusieron políticas de seguridad (66 %), mientras que el Reino Unido obtuvo el porcentaje más bajo (42 %). Los sectores regulados impusieron políticas (64-66 %) en un porcentaje muy superior a la media internacional del 55 %. En España se produjo el mayor aumento en el número de empresas que impusieron políticas de seguridad, alcanzando un 48 % desde un 40 %.

RECOMENDACIÓN:

Garantizar el cumplimento de las políticas es igual de importante que crear la política en primera instancia. Las organizaciones deben asegurarse de tener una metodología para que los dispositivos que no cumplan con las políticas vuelvan a hacerlo o, si no, evitar que estos puedan acceder a todos los recursos. Por ejemplo, si un dispositivo infringe una política de código de acceso, el departamento informático podrá impedir al usuario que acceda a las aplicaciones y datos corporativos en dicho dispositivo hasta que se cumplan los requisitos del código de acceso.

PORCENTAJE DE EMPRESAS QUE IMPONEN POLÍTICAS DE SEGURIDAD



MobileIron

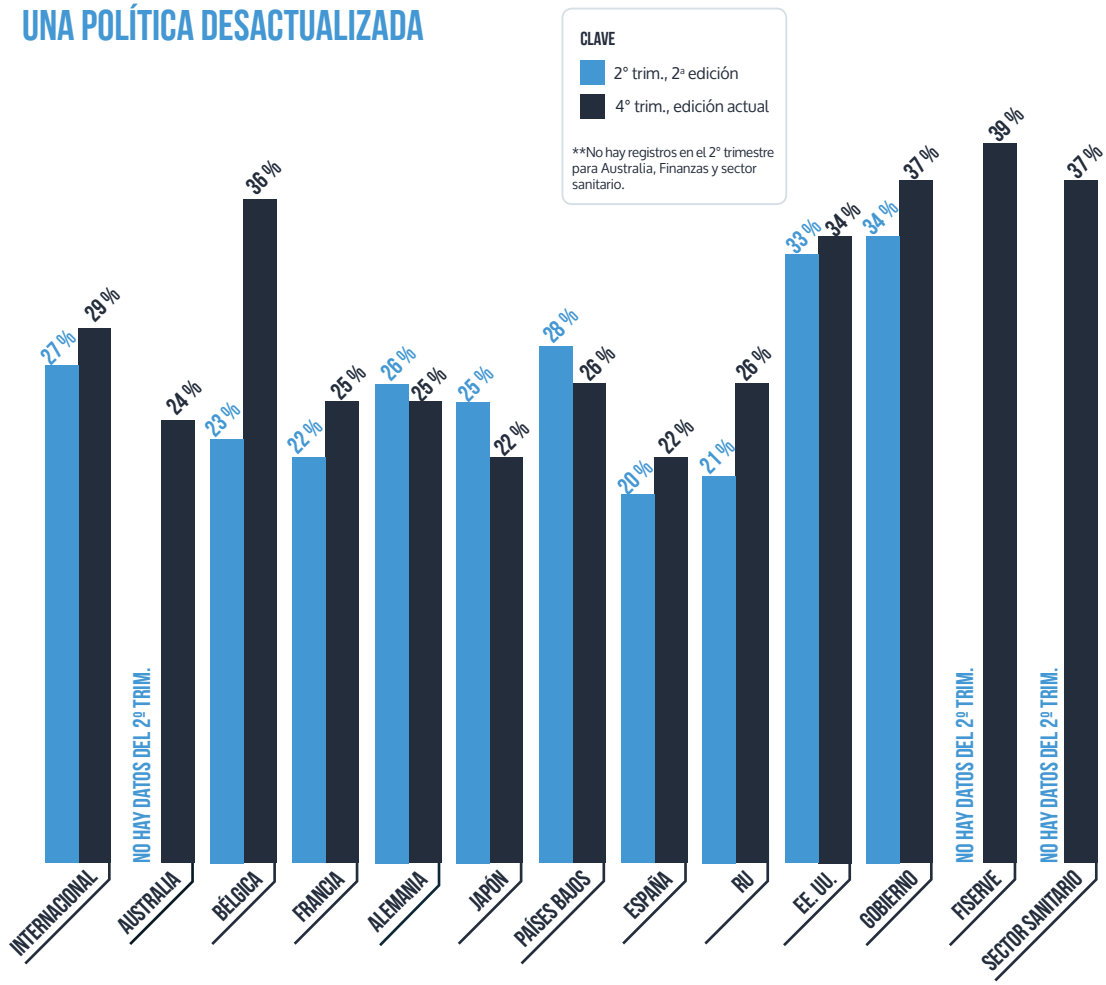
POLÍTICAS DESACTUALIZADAS

Casi un 30 % de las empresas tienen al menos una política desactualizada, una tendencia que no se ha modificado demasiado desde el informe anterior. Las políticas desactualizadas se dan cuando el administrador de tecnologías móviles modifica una política en la consola, pero dicho cambio no se propaga a todos los dispositivos administrados. Esto suele ser resultado del comportamiento del usuario. Por ejemplo, puede ocurrir que los usuarios tengan un dispositivo que utilizan con poca frecuencia o que reciban un dispositivo nuevo y dejen de utilizar el anterior. Esto provoca situaciones en las que un dispositivo se conecta con poca frecuencia o «va desapareciendo», evitando que reciba actualizaciones. La mayoría de las regiones observaron un aumento del porcentaje de empresas con políticas desactualizadas, aunque Alemania, Japón y los Países Bajos sufrieron un descenso. España y Japón son los países con menos políticas desactualizadas (ambos con un 22 %), mientras que en Bélgica es donde más hay, con un 36 %. De hecho, en Bélgica se pasó de un 23 % en el 2° trimestre a un 36 % en el 4° trimestre. Los tres sectores tenían tasas de políticas desactualizadas superiores a la mayoría de las regiones individuales.

RECOMENDACIÓN:

Como los dispositivos con políticas desactualizadas no cumplen con el estándar de configuración actual, el departamento informático debe configurar la plataforma de administración para que notifique automáticamente a los usuarios y les proporcione los pasos para actualizar rápidamente las políticas y configuraciones desactualizadas. Dependiendo de los requisitos de seguridad, puede que el departamento informático considere restringir el acceso de dispositivos a los recursos corporativos hasta que el problema se haya diagnosticado y resuelto.

PORCENTAJE DE EMPRESAS CON AL MENOS UNA POLÍTICA DESACTUALIZADA



«CASI EL 30 % DE LAS EMPRESAS TIENEN AL MENOS UNA POLÍTICA DESACTUALIZADA»

MobileIron

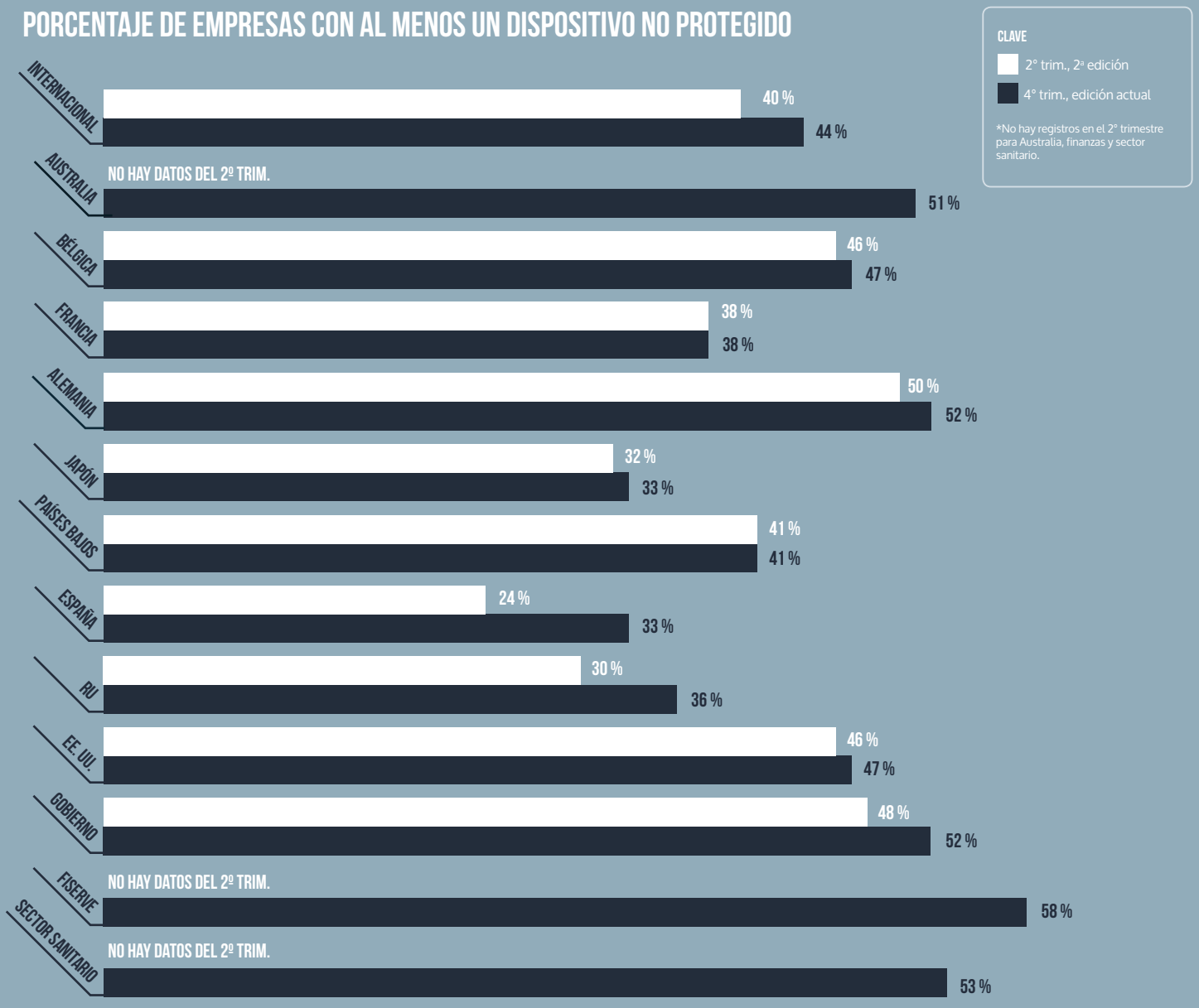
DISPOSITIVOS NO PROTEGIDOS

El porcentaje de empresas con al menos un dispositivo no protegido aumentó del 40 % al y 44 % en todo el mundo. Esto se puede atribuir en parte la expansión de la movilidad corporativa internacional y al mayor número de dispositivos móviles bajo administración corporativa pero, no obstante, las implicaciones son sumamente graves. Cuando un dispositivo corporativo se roba o se pierde, la empresa se arriesga a perder mucho más que solamente el coste del hardware. Si los datos corporativos, como los datos personales de empleados o clientes, datos financieros de la empresa u otra información confidencial cae en las manos equivocadas, la organización puede enfrentarse a inmensos costes legales, monetarios y de reputación. Cada región, a excepción de Francia y los Países Bajos, sufrió un aumento del porcentaje de empresas con al menos un dispositivo no protegido. España fue el país con un mayor porcentaje de empresas en las que se perdió al menos un dispositivo móvil: de un 24 % a un 33 %. Más de la mitad de todos los sectores tenían al menos una empresa con un dispositivo no protegido. Servicios financieros fue el sector con más incidencias en este sentido, con un 58 %.

RECOMENDACIÓN:

Las empresas siempre tendrán que enfrentarse a la pérdida o robo de dispositivos, pero la pérdida de datos sí es algo que se puede evitar. Las organizaciones deberían tener una solución de EMM instaurada que permita al departamento informático borrar de forma remota datos y aplicaciones corporativos de dispositivos robados o perdidos. La capacidad de hacer un seguimiento remoto de un dispositivo perdido y denegar el acceso a los usuarios no autorizados también es una función fundamental para garantizar que, aunque el dispositivo caiga en las manos equivocadas, los datos no lo estén nunca.

PORCENTAJE DE EMPRESAS CON AL MENOS UN DISPOSITIVO NO PROTEGIDO



MobileIron

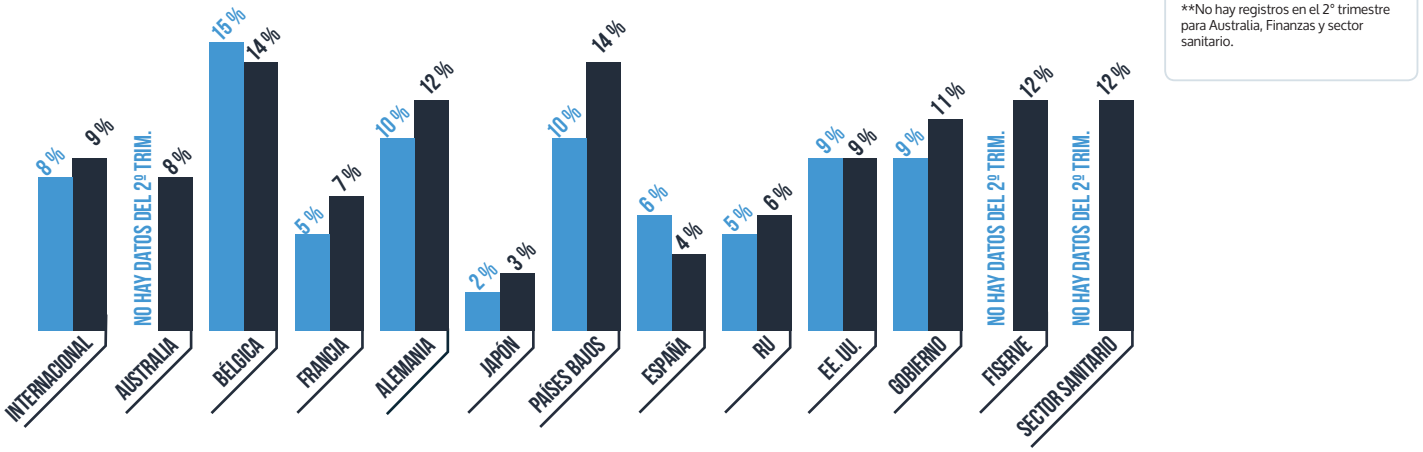
IMPOSICIÓN DE LAS ACTUALIZACIONES DEL SISTEMA OPERATIVO

Los proveedores de SO saben que los hackers tienen en el punto de mira los dispositivos móviles y aplicaciones. Estas amenazas siguen evolucionando rápidamente, de forma que los proveedores están trabajando cada vez más para ofrecer revisiones de seguridad en forma de actualizaciones del sistema operativo con el fin de proteger a los usuarios y los datos de los ataques más recientes. Obviamente, para ser eficientes, estas actualizaciones deben instalarse. Por suerte, en 2016 se produjo una tendencia positiva en esta dirección. La mayoría de las regiones y verticales observaron un aumento en el porcentaje de empresas que imponían actualizaciones de los SO. Las industrias centradas en la seguridad, como los servicios financieros (12 %), las administraciones (11 %) y el sector sanitario (12 %) están implementando actualizaciones del SO a una velocidad muy superior a la media internacional del 9 %. Las empresas belgas y holandesas (ambas con un 14 %) fueron las que más actualizaciones del sistema operativo implementaron. Las que menos, fueron las empresas japonesas (3 %).

RECOMENDACIÓN:

La imposición de actualizaciones del SO es una de las formas más sencillas y rentables de evitar ataques procedentes de agujeros de vulnerabilidad en sistemas operativos más antiguos. Las revisiones de seguridad abordan estas vulnerabilidades específicas y, como resultado, la imposición de SO actualizados proporciona una de las mejores protecciones frente a amenazas móviles. Por muy poco esfuerzo e inversión, las revisiones ofrecen una gran ventaja en lo referente a la seguridad. En el caso de dispositivos iOS, la supervisión del DEP de Apple simplifica este proceso. Si el dispositivo funciona con iOS 9 o superior y está supervisado de forma inalámbrica mediante el programa DEP de Apple, una plataforma de EMM puede provocar descargas y actualizaciones del último lanzamiento de iOS. Sencillamente, no hay motivo para no garantizar que los sistemas operativos estén constantemente actualizados. Piense en la regla del 80/20: las organizaciones pueden cosechar un 80 % de beneficios con tan solo un 20 % del esfuerzo.

PORCENTAJE DE EMPRESAS QUE IMPONEN ACTUALIZACIONES DEL SO



MobileIron

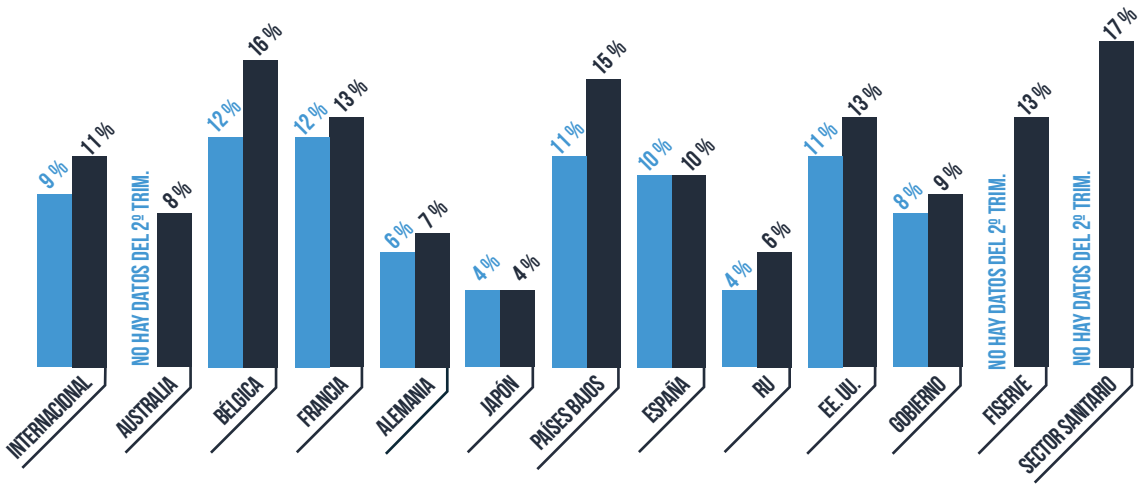
DISPOSITIVOS AFECTADOS

Los usuarios están siempre buscando la forma de obtener las aplicaciones y contenidos móviles que necesitan para hacer su trabajo, aunque esto a veces suponga sortear los controles de seguridad. Con Android, siempre ha habido herramientas para descifrar el dispositivo, mientras que iOS requiere un software de «jailbreak» si se desean omitir ciertos controles de seguridad. Aunque Pangu, el fabricante de algunas de las herramientas de «jailbreak» más conocidas, ofreció actualizaciones inmediatamente después del lanzamiento inicial de iOS 9, Apple fue rápido al lanzar una revisión y, posteriormente, las actualizaciones de Pangu no estuvieron disponibles hasta que iOS 10 estuvo en versión beta. A pesar de esta «sequía», la tasa de dispositivos a los que se les realizó un «jailbreak» ha seguido aumentando. La proporción de dispositivos afectados pasó de un 9 % a un 11 % a nivel internacional. Los servicios financieros (13 %) y el sector sanitario (17 %) experimentaron mayores tasas de dispositivos afectados que la administración (9 %). Con solo un 4 %, las empresas japonesas son las que menos incidentes tuvieron con dispositivos afectados.

RECOMENDACIÓN:

Tras la revisión, la medida de seguridad más importante que las organizaciones tecnológicas pueden tomar es garantizar el cumplimiento de los dispositivos. Con la solución de EMM adecuada, el departamento informático puede evitar que los dispositivos afectados o que no cumplan las políticas puedan acceder a los recursos corporativos hasta que problema se haya resuelto. Es fundamental evitar que los dispositivos estén en peligro para mantener los datos corporativos seguros, ya que los dispositivos descifrados o con «jailbreaks» son sumamente vulnerables a los ataques.

PORCENTAJE DE EMPRESAS CON AL MENOS UN DISPOSITIVO AFECTADO



CLAVE

2° trim., 2a edición

Cifras actuales

*No hay registros en el 2° trimestre para Australia, finanzas y sector sanitario.

MobileIron

CIBERHIGIENE

El malware móvil ha evolucionado más allá de la filtración de datos y ahora es capaz de afectar a todo el dispositivo. Aunque los dispositivos móviles tiene muchas funciones de seguridad inherentes, como el sistema de contenedores aislados, algunos tipos de ataques pueden omitir estas características. Estos tipos de malware son eficaces en quitar el control al usuario y ponerlo en manos del atacante.

A pesar del aumento en ataques de malware móvil de alto perfil, la adopción de antimalware continúa siendo la misma, con una tasa de adopción internacional por debajo del 5 %.

Aunque algunos tipos de ataques de malware móvil son difíciles de propagar a escala masiva (de momento), los departamentos informáticos deben mantener una buena ciberhigiene para proteger sus aplicaciones y datos corporativos ante una nueva oleada de ataques de malware móvil. Algunas de las prácticas de ciberhigiene más eficaces son sencillas y muy rentables de implementar, por lo que deberían formar parte del kit básico de herramientas de cualquier organización tecnológica.

LISTA DE PRIORIDADES DE LA CIBERHIGIENE

1. CONTROLAR LAS PRÁCTICAS DE RIESGO DEL USUARIO.

El comportamiento arriesgado de los empleados es cada vez más habitual. En todo el mundo, el 11 % de las empresas tenían al menos un dispositivo afectado que podía acceder a datos corporativos en el 4° trimestre y hasta un 9 % en el 2° trimestre. Además, el 44 % de las empresas notificaron que les faltaba algún dispositivo, hasta un 40 % en el 2° trimestre. Para protegerse contra el acceso no autorizado a los recursos corporativos, los departamentos informáticos deben mejorar la aplicación de políticas y el cumplimiento de los dispositivos. No obstante, cuando el departamento informático intenta imponer políticas de seguridad, pueden crear pasos adicionales que los usuarios intentarán sortear tomando medidas no autorizadas como descifrar o hacer un «jailbreak» en sus dispositivos. Administrar dispositivos «con mano dura» no es la mejor forma de enfocar la seguridad móvil pero, para garantizar algunas medidas de protección de los servicios corporativos, debe verificarse con frecuencia el estado de seguridad de los dispositivos y las aplicaciones.

2. GARANTIZAR QUE EL SISTEMA OPERATIVO ESTÉ SIEMPRE ACTUALIZADO.

Si bien las tendencias de ciberseguridad corporativa se mantuvieron por lo general inalterables entre el 2° y el 4° trimestre de 2016, las áreas tecnológicas sí aumentaron su imposición de actualizaciones del sistema operativo para garantizar la implementación de las revisiones críticas de seguridad llevadas a cabo en los dispositivos corporativos móviles. Garantizar la aplicación de las actualizaciones del sistema operativo es un proceso que requiere poco esfuerzo y es muy eficaz para garantizar la protección de los dispositivos frente a las constantes amenazas de seguridad. Las revisiones son una de las prácticas de ciberseguridad más básicas y sencillas. A pesar de ello, solo el 9 % de las empresas impusieron revisiones en el 4° trimestre. El motivo de este porcentaje tan bajo puede ser debido a que las empresas todavía no han puesto en práctica esta medida de seguridad básica en sus implementaciones móviles. Las organizaciones deberían exigir que los sistemas operativos [de los dispositivos] no sean anteriores a la segunda versión más actual, incluidas las versiones y revisiones secundarias. Por ejemplo, si la última versión de Apple iOS es 10.2, no se debería permitir que ningún dispositivo con una versión anterior a iOS 10.1.1 accediera a los recursos corporativos. El lanzamiento y programación de las actualizaciones de Android es ligeramente diferente y, por tanto, el enfoque a la hora de supervisar versiones de Android puede variar. Como regla general, las versiones anteriores de Android siguen recibiendo actualizaciones de seguridad durante un período de al menos tres años desde su lanzamiento inicial, mientras que los grandes lanzamientos se lanzan anualmente. En el momento de redactar este informe, las versiones Android v7.0 etc eran todas ellas de uso generalizado, y Android v7.0 también estaba disponible al gran público[7]. Android también se ha pasado a un ciclo mensual de lanzamientos de revisiones de seguridad. A pesar de las grandes variaciones en las versiones del SO y niveles de revisión, es aplicable en la misma lógica N-1 básica: por cada versión de Android en un entorno, los dispositivos deberían tener como mínimo la última versión principal/secundaria y un nivel de revisión de seguridad que no lleve desactualizado más de un mes. Por ejemplo, los dispositivos deben incluir v4.4.4, v5.1.1, v6.0.1 o v7.1.1 y deben disponer de un nivel de revisión de seguridad no anterior al 01/12/2016 o al 05/12/2016. Hay que tener en cuenta que Google no ofrece actualmente actualizaciones de seguridad para versiones de Android anteriores a la v4.4.4, de modo que puede ser necesaria la aplicación de medidas adicionales para garantizar la integridad del dispositivo y la seguridad de sus datos.

[7] Fuente: https://developer.android.com/about/dashboards/index.html

3. DENEGAR EL ACCESO DESDE LOS DISPOSITIVOS AFECTADOS.

Los sistemas operativos afectados son desde hace mucho tiempo uno de los principales objetivos de los atacantes móviles, ya que sortean importantes características de seguridad convirtiéndolos en blancos fáciles. Actualmente, estamos observando una tendencia emergente del malware móvil que incorpora vulneraciones para poner en riesgo el sistema operativo sin que el usuario sea consciente de ello. A medida que esta tendencia avanza, el riesgo de estas vulnerabilidades cambia desde casos aislados impulsados por acciones del usuario hasta ataques más amplios provocados por actores más organizados. En el momento actual, las empresas con al menos un dispositivo afectado que intentaba acceder a datos corporativos aumentaron desde un 9 % a un 11 % en todo el mundo. Las organizaciones deben asegurarse de tener los dispositivos afectados bajo control y bloquear el acceso a todos los recursos corporativos desde estos dispositivos.

4. EVITAR LA CONFIGURACIÓN Y LAS MODIFICACIONES DE APLICACIONES.

Muchas amenazas de seguridad móvil se originan con ingeniería social y técnicas diseñadas para engañar a los usuarios y lograr que instalen configuraciones malignas, software o ambos. Estas amenazas a menudo se originan en fuentes no autorizadas como sitios web o app stores de terceros. Las organizaciones deberían controlar las configuraciones y aplicaciones de carga en paralelo supervisando la configuración «no administrada» y los perfiles de aprovisionamiento en iOS. En el caso de Android, si se desactiva la opción «Permitir fuentes que no sean de confianza» y se supervisan los permisos de las aplicaciones (por ejemplo, bloqueando aplicaciones que soliciten el permiso del administrador del dispositivo), se reducirá el riesgo de cambios no autorizados en las configuraciones y aplicaciones. No obstante, las últimas investigaciones muestran que, mientras que la mayoría de las organizaciones dedican tiempo a crear políticas, casi la mitad de las empresas encuestadas no toma ninguna medida, como por ejemplo bloquear el acceso a la red. Esto puede deberse a que, en muchas situaciones de bajo riesgo, la medida consiste únicamente en alertar al empleado o al administrador informático para solicitar una solución manual. No obstante, la solución manual no es inmediata ni requiere que empleado tome ninguna medida correctiva. Por lo tanto, nuestra recomendación es automatizar la imposición de políticas. Para ello, las organizaciones deberán actualizar de un modo uniforme todas las políticas para protegerse frente a futuros ataques móviles.

ADOPCIÓN DEL PCV Y EL DEP

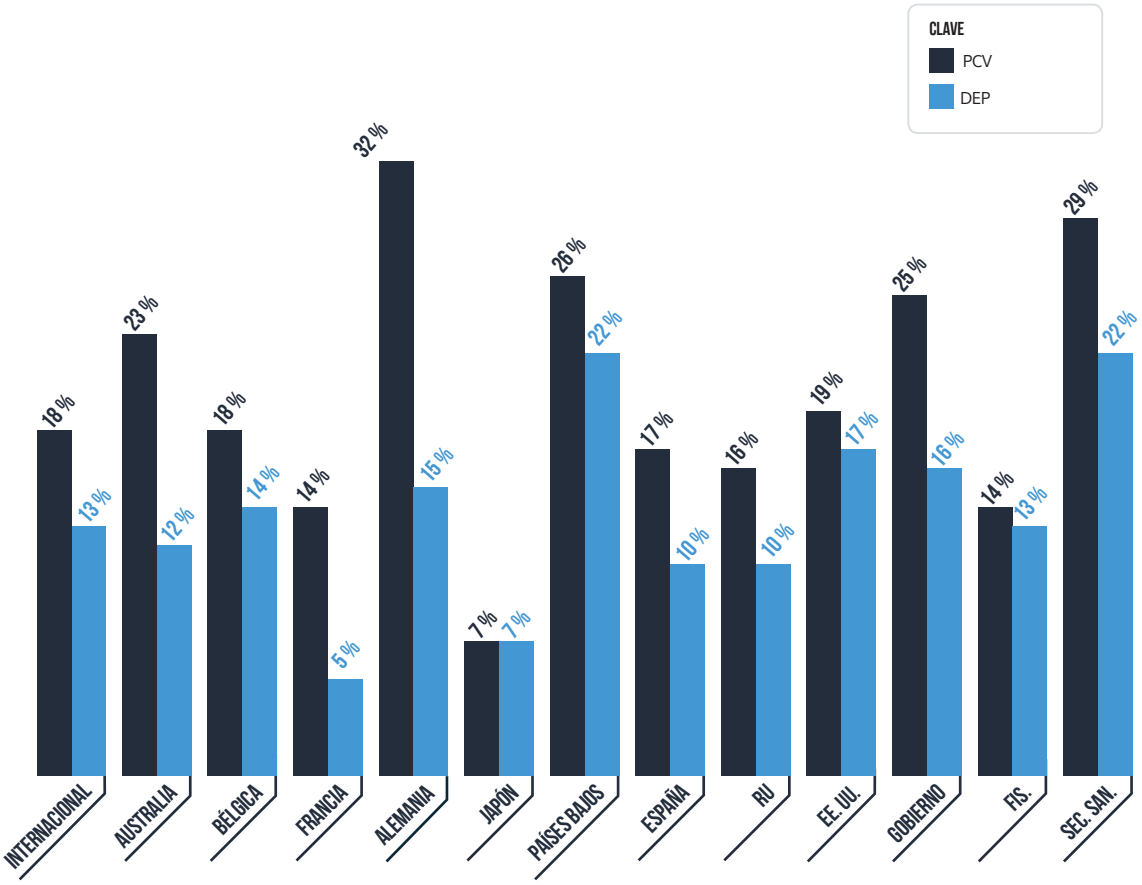
Por primera vez, este informe midió la adopción internacional del Programa de Inscripción de Dispositivos (DEP) y el Programa de Compras por Volumen (PCV) de Apple.

El PCV se lanzó en 2011 y alcanzó su punto álgido con la introducción del programa de flotas corporativas DEP ya que, juntos, ofrecen a las organizaciones las herramientas para administrar flotas de dispositivos iOS y las aplicaciones que sobre estos se ejecutan.

Casi una de cada cinco organizaciones (18 %) está utilizando actualmente el PCV para simplificar la implementación de aplicaciones corporativas para los usuarios. Esta tasa es considerablemente superior en el sector sanitario (29 %) y la administración (25 %). Con un 32 %, Alemania es el país donde más organizaciones utilizan el PCV. Con solo un 7 %, las empresas japonesas son las que menos utilizan el PCV.

Además, las organizaciones están aumentando su adopción del DEP porque les proporciona un mayor control sobre sus flotas móviles. Con el DEP, las empresas pueden implementar mayores restricciones en dispositivos supervisados propiedad de la empresa. Por ejemplo, se pueden restringir las tablets al modo kiosco de una sola aplicación («single-app») para evitar que los usuarios descarguen aplicaciones no autorizadas. Actualmente, casi el 13 % de las organizaciones de todo el mundo está utilizando el DEP. Las empresas de los Países Bajos registraron el mayor uso del DEP con un 22 %, mientras que sus homólogos franceses cifraron las tasas más bajas con solo un 5 %. Casi un cuarto (22 %) de las organizaciones del sector sanitario está utilizando actualmente el DEP.

PORCENTAJE DE EMPRESAS QUE UTILIZAN EL PCV Y EL DEP



MobileIron

ESTADO DE LAS APLICACIONES CORPORATIVAS

CUATRO DE CADA CINCO ORGANIZACIONES TIENEN 10 APLICACIONES O MÁS

Casi el 80 % de las empresas tienen más de 10 aplicaciones corporativas instaladas. Las organizaciones en los Países Bajos (90 %) son las que tienen la mayor probabilidad de tener una media de más de 10 aplicaciones instaladas, mientras que las organizaciones en Japón (71 %) son las que tienen una menor probabilidad. Esta tasa también es alta en los sectores verticales. Entre las organizaciones de servicios financieros, el 88 % tenía una alta probabilidad de contar con más de 10 aplicaciones instaladas, seguidas de cerca por la administración 83 % y el sector sanitario 82 %.

PORCENTAJE DE EMPRESAS CON MÁS DE 10 APLICACIONES INSTALADAS

MobileIron

LAS APLICACIONES MÁS INSTALADAS

	INTERNACIONAL	AUSTRALIA	FRANCIA	ALEMANIA	JAPÓN	BÉLGICA	PAÍSES BAJOS
1	Webex	AnyConnect	File Manager	Arm	Google Maps	Touchdown	Chrome
2	AnyConnect	LinkedIn	WIT Mobile	Keynote	Webex	Pulse Secure	Whatsapp
3	Concur	Edge	Canet	Numbers	Chrome	Webex	Word
4	Adobe Acrobat	VIP Access	MA Banque	Pages	Salesforce	Pages	Adobe Acrobat
5	Pulse Secure	Entertain	Annuaire	Adobe Acrobat	Smart Catalog	ECAS Mobile	QuickSupport for Samsung
6	Keynote	Telstra 24x7	Ma Carte	Excel	Web Directory	Evernote	YouTube
7	Numbers	Chrome	Google Maps	DB Navigator	box	Word	Excel
8	Pages	Google Maps	Les Infos	Word	Jabber	Excel	LinkedIn
9	Google Maps	Citrix Receiver	Adobe Acrobat	Companion	Word	Salesforce	Google Maps
10	Word	Concur	Smart TPE	Webex	Powerpoint	File Manager	Evernote

	ESPAÑA	RU	EE. UU.	GOBIERNO	FISERVE	SECTOR SANITARIO
1	Numbers	Chrome	Webex	Adobe Acrobat	Webex	Webex
2	Keynote	Google Maps	Concur	Pages	Ma Banque	Concur
3	iMovie	Adobe Acrobat	AnyConnect	AnyConnect	Canet	Pulse Secure
4	Alertas	Word	Adobe Acrobat	Numbers	RSA SecureID Software Token	AnyConnect
5	Whatsapp	Excel	Pulse Secure	Keynote	Adobe Acrobat	Keynote
6	Pulse Secure	Keynote	Jabber	Pulse Secure	Pulse Secure	Excel
7	Citrix Receiver	Gmail	box	Google Maps	Google Maps	Word
8	Kaspersky Endpoint Security	YouTube	Keynote	YouTube	Citrix Reciever	Powerpoint
9	Microstrategy	Nervecentre	Numbers	RSA SecureID Software Token	Any Connect	box
10	YouTube	Pages	Pages	Evernote	Word	Numbers

LAS APLICACIONES MÁS BLOQUEADAS

La lista de aplicaciones más bloqueadas podría considerarse un distintivo honorífico para las aplicaciones del consumidor más populares que han captado la atención de los equipos de seguridad informáticos. Debido a su extendido uso y al riesgo percibido que pueden suponer, las organizaciones de todo el mundo está bloqueando cada vez más aplicaciones como WhatsApp, Netflix y Outlook, además de las clásicas como Angry Birds y Twitter. Otras aplicaciones, como Evernote, Box y Line, han salido de la lista, en parte debido a su uso cada vez mayor por parte de las empresas.

LISTA NEGRA DE LAS APLICACIONES MÁS BLOQUEADAS

	INTERNACIONAL	AUSTRALIA	BÉLGICA	FRANCIA	ALEMANIA	JAPÓN	PAÍSES BAJOS
1	Angry Birds	Angry Birds	Facebook	Facebook	Dropbox	Line	Dropbox
2	Dropbox	Facebook	Dropbox	Angry Birds	Facebook	Dropbox	CamScanner
3	Facebook	Hipster Pawslez	WeChat	Dropbox	Whatsapp	Evernote	Cydia
4	Whatsapp	path	Angry Birds	Twitter	Angry Birds	Skype	Winzip
5	Twitter	Dropbox	PDF Reader	Outlook	OneDrive	Team Viewer	CamCard
6	Skype	Twitter	Winzip	Cydia	Outlook	Twitter	OPlayer
7	OneDrive	2Day FM	Google Drive	Candy Crush	Google Drive	One Drive	WeChat
8	Outlook	Pandora	CamCard	YouTube	Twitter	Facebook	Outlook
9	Netflix	xCon	Mercury	Clash of Clans	Sugarsync	Viber	PDF Reader
10	Google Drive	Google Drive	Twitter	Skype	Skype	Tunnelbear	Mobile Ticket

	ESPAÑA	RU	EE. UU.	GOBIERNO	SECTOR SANITARIO	FISERVE
1	Angry Birds	Dropbox	Angry Birds	Angry Birds	Angry Birds	Dropbox
2	Facebook	Angry Birds	Dropbox	Dropbox	Dropbox	Angry Birds
3	Twitter	Facebook	Facebook	Facebook	Facebook	Facebook
4	YouTube	Twitter	Netflix	Outlook	Netflix	Outlook
5	Pokemon GO	Whatsapp	Pandora	Whatsapp	Twitter	box
6	Cydia	box	Outlook	box	Outlook	Twitter
7	Viber	Outlook	box	Cydia	Skype	Instagram
8	Soduku	OneDrive	Twitter	Snapchat	Google Drive	Sugarsync
9	Powerpoint	Skype	YouTube	vShare App Market	OneDrive	box
10	LINE	SugarSync	OneDrive	Google Drive	Whatsapp	YouTube

SECTOR A DESTACAR: LA ADMINISTRACIÓN

Las administraciones de todo el mundo se ven a menudo paralizadas por la burocracia y los problemas de financiación. Con frecuencia suelen tener problemas para contratar y mantener a su personal, poner en marcha las tecnologías y mantenerlas actualizadas de forma puntual. A pesar de todos estos obstáculos, los departamentos de informática de las administraciones están manteniendo, por lo general, buenas prácticas de ciberhigiene. No obstante, los usuarios de las administraciones son más permisivos y su falta de vigilancia puede poner en riesgo los datos oficiales en sus dispositivos móviles.

PRÁCTICAS DE CIBERHIGIENE:

LA IMPOSICIÓN DE ACTUALIZACIONES DEL SO HA AUMENTADO DESDE EL 9 % EN EL 2º TRIMESTRE HASTA UN

11 %

EN EL 4º TRIMESTRE

25 %

UTILIZA EL PCV

16 %

UTILIZA DEP

63 %

IMPUSO POLÍTICAS EN EL 4º TRIMESTRE. HASTA EL 61 % EN EL 2º TRIMESTRE

37 %

TENÍA POLÍTICAS DESACTUALIZADAS EN EL 4º TRIMESTRE. HASTA UN 34 % EN EL 2º TRIMESTRE

75 %

HABÍA APLICADO MÁS DE UNA POLÍTICA DE SEGURIDAD EN EL 4º TRIMESTRE. SIN CAMBIOS CON RESPECTO AL 2º TRIMESTRE

43 %

HABÍA APLICADO MÁS DE UNA POLÍTICA APPCONNECT EN EL 4º TRIMESTRE. SE REDUJO DESDE UN 45 % EN EL 2º TRIMESTRE

COMPORTAMIENTO DE RIESGO POR PARTE DEL USUARIO:

9 %

TENÍA UN DISPOSITIVO AFECTADO QUE ACCEDÍA A DATOS CORPORATIVOS EN EL 4º TRIMESTRE. HASTA UN 8 % EN EL 2º TRIMESTRE

AL **52 %**

LES FALTABAN DISPOSITIVOS EN EL 4º TRIMESTRE. HASTA UN 38 % EN EL 2º TRIMESTRE

SECTOR A DESTACAR: SECTOR SANITARIO

El DEP hace que la administración de dispositivos sea obligatoria, resultando idónea para imponer las políticas de seguridad en dispositivos propiedad de la empresa. Las organizaciones sanitarias han comenzado a utilizar DEP y el PCV para proteger los datos especialmente confidenciales de sus pacientes y cumplir las normativas implementando automáticamente controles de seguridad proactivos. Si bien el uso de DEP y el PCV son medidas positivas de seguridad, las organizaciones sanitarias pueden mejorar otras áreas de la ciberhigiene y los comportamientos de riesgo de los usuarios.

PRÁCTICAS DE CIBERHIGIENE:

LAS EMPRESAS DEL SECTOR SANITARIO SON LAS QUE TIENEN MAYORES PROBABILIDADES DE UTILIZAR EL DEP (22 %) Y EL PCV (29 %).

29 %
PCV

22 %
DEP

64 %
IMPONE POLÍTICAS

PERO SOLO EL
12 %
IMPONE LAS ACTUALIZACIONES DE SISTEMAS OPERATIVOS

37 %
TENÍA POLÍTICAS DESACTUALIZADAS

77 %
TENÍA MÁS DE UNA POLÍTICA DE SEGURIDAD

41 %
TENÍA MÁS DE UNA POLÍTICA APPCONNECT

COMPORTAMIENTO DE RIESGO DEL USUARIO:

17 %
DE LAS ORGANIZACIONES DEL SECTOR SANITARIO TUVIERON AL MENOS UN DISPOSITIVO AFECTADO QUE ACCEDÍA A DATOS CORPORATIVOS. EL PORCENTAJE MÁS ALTO DE TODA LA MUESTRA.

53 %
NOTIFICARON DISPOSITIVOS AFECTADOS

SECTOR A DESTACAR: LOS SERVICIOS FINANCIEROS

Las empresas de servicios financieros tenían las tasas de adopción más bajas del DEP y el PCV. Teniendo en cuenta los requisitos normativos de este sector, el DEP y el PCV ofrecen muchas ventajas para lograr el cumplimiento. Estas organizaciones también pueden mejorar en otras áreas de ciberhigiene y comportamiento de riesgo del usuario.

PRÁCTICAS DE CIBERHIGIENE:

SOLO EL

14 %

UTILIZA EL PCV

Y

13 %

UTILIZA DEP

ESTA TASA DE ADOPCIÓN ES INFERIOR A LAS TASAS DEL SECTOR SANITARIO Y DE LA ADMINISTRACIÓN

66 %

IMPONE POLÍTICAS

PERO SOLO EL

12 %

IMPONE LAS ACTUALIZACIONES DE SISTEMAS OPERATIVOS

39 %

TENÍA POLÍTICAS DESACTUALIZADAS

78 %

TENÍA MÁS DE UNA POLÍTICA DE SEGURIDAD

49 %

TENÍA MÁS DE UNA POLÍTICA APPCONNECT

COMPORTAMIENTO DE RIESGO DEL USUARIO:

13 %

TENÍA AL MENOS UN DISPOSITIVO AFECTADO QUE ACCEDÍA A DATOS CORPORATIVOS

58 %

TENÍA DISPOSITIVOS AFECTADOS

CONCLUSIONES Y RECOMENDACIONES

A la vista de estos resultados, las organizaciones deberían tener en cuenta las siguientes recomendaciones generales para mejorar su seguridad móvil:

1. CONTROLAR LOS COMPORTAMIENTOS DE RIESGO DEL USUARIO.

Es fundamental garantizar el cumplimiento de los dispositivos para evitar que los no autorizados accedan a recursos corporativos críticos. Además, es probable que servicios como aplicaciones web, Wi-Fi corporativa y VPN requieran configuraciones adicionales y aplicación de políticas para evitar el acceso desde dispositivos no autorizados.

2. IMPONER ACTUALIZACIONES DEL SO.

Las organizaciones deberían exigir que los sistemas operativos no sean anteriores a la segunda versión más actual, incluidas las versiones y revisiones secundarias. Por ejemplo, si la última versión de Apple iOS es 10.2, no se debería permitir que ningún dispositivo con una versión anterior a iOS 10.1.1 accediera a los recursos corporativos. El lanzamiento y programación de las actualizaciones de Android es ligeramente diferente y, por tanto, el proceso de supervisión de las diferentes versiones de Android podría variar.

3. DENEGAR EL ACCESO DESDE SISTEMAS OPERATIVOS AFECTADOS.

Las organizaciones no pueden limitarse a crear políticas, sino que tienen que imponer y actualizar siempre las políticas de seguridad en todos los dispositivos que accedan a los recursos corporativos. A los dispositivos que no cumplan con las políticas en vigor se les debe negar el acceso o deben estar obligados a seguir rápidamente los pasos para su cumplimiento.

4. EVITAR O SUPERVISAR LA CONFIGURACIÓN Y LA CARGA ADICIONAL DE APLICACIONES.

Las organizaciones deben utilizar herramientas de gestión para garantizar que los usuarios no puedan instalar manualmente perfiles de configuración o aprovisionamiento, evitando así hábitos peligrosos, como pulsar un enlace para instalar certificados o aplicaciones internas que pueden ser utilizadas por atacantes. Asimismo, las organizaciones deben utilizar sus herramientas de administración para garantizar que los usuarios no hayan omitido las protecciones del SO para evitar la carga adicional / paralela de aplicaciones, como la habilitación de fuentes «que no sean de confianza» en Android, o permitir que perfiles de aprovisionamiento desconocidos resulten de confianza para iOS.

5. UTILIZAR LAS FUNCIONES DE SEGURIDAD QUE OFRECEN LOS PROGRAMAS PROPIEDAD DE LAS EMPRESAS.

A medida que los casos de las empresas van siendo cada vez más habituales, los proveedores de sistemas operativos móviles han empezado a ampliar las herramientas para mejorar la «experiencia del usuario» de las empresas. El Programa de inscripción de dispositivos (DEP) de Apple y el Modo Propietario del Dispositivo de Google Android proporcionan a las organizaciones funciones adicionales para segurizar sus flotas de dispositivos móviles, como la inscripción obligatoria de EMM y opciones adicionales de restricción y configuración.

METODOLOGÍA

La información contenida en este informe está basada en datos anónimos normalizados, recogidos entre el 1 de octubre y el 31 de diciembre de 2016. Pensamos que se trata del mayor estudio sobre seguridad en dispositivos móviles específicos para empresas realizado hasta el momento, en los tres sistemas operativos móviles más comunes: Android, etc.