GUÍA TECNOLÓGICA

Seguridad Móvil

Una perspectiva global sobre aspectos emergentes de la seguridad de los dispositivos móviles.

- AMENAZAS:
  Malware, pérdida o robo de dispositivos, amenazas principales a la seguridad de los teléfonos móviles

- MDM:
  El mercado de gestión de dispositivos móviles ofrece opciones para la seguridad de estos equipos

- SAAS:
  Emergen las opciones de seguridad SaaS como defensa ante los riesgos de seguridad de los dispositivos móviles

- TABLETAS:
  ¿Preocupado por la seguridad de las tabletas? Algunos lo están; otros, no tanto

- BYOD:
  Seguridad 'trae tu propio dispositivo': ¿Qué opina India Inc.?

TechTarget

Malware, pérdida o robo de dispositivos, amenazas principales a la seguridad de los teléfonos móviles

Descubre las amenazas principales que están surgiendo contra los teléfonos móviles usados en tu organización.

POR HILLARY O'ROURKE

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

ANTE EL aumento exponencial de quienes se lanzan en tropel a conseguir el último smartphone, los expertos anuncian que es simplemente una cuestión de tiempo hasta que los cibercriminales decidan trasladarse también a este terreno. Y advierten que las amenazas a las que se enfrenta la seguridad de los teléfonos móviles de nueva generación—amenazas que los creadores de malware tardaron décadas en llevar a las computadoras—son tan sofisticadas que son capaces de atacar a las plataformas móviles actuales en tan sólo unos pocos meses.

Con el ataque preciso, los cibercriminales tienen la posibilidad de acceder a la información corporativa y a los emails que contienen dicha información a través de un dispositivo móvil, dice Toralv Dirro, especialista en estrategias de seguridad para Europa, Medio Oriente y África (EMEA) de McAfee Inc.

"Muchas compañías no cuentan con los medios tecnológicos y las políticas para [garantizar] la seguridad de estos dispositivos móviles," dice Dirro. "Es un terreno todavía sin explorar."

Las empresas de seguridad no dudan en aseverar que, si bien 2011 fue el año de las amenazas a las plataformas móviles, a este paso, 2012 puede batir el récord. Investigadores de la compañía de seguridad M86 Security Inc. dicen que, este año, el malware para dispositivos móviles será "una de las áreas más preocupantes de explotación criminal." Según el informe de M86 Security "Threats Predictions of 2012" (.pdf), en 2011 las muestras de malware móvil no controladas se calculaban en más de 2.500. Sin embargo, esa cifra rápidamente superó las 7.500 muestras.

"Con base en [2011], éste es algo así como el año del malware de Android," dice Patrik Runald, gerente principal de investigación sobre seguridad en la empresa Websense Inc., radicada en San Diego, California. "Puedo vaticinar con bastante seguridad que eso va a continuar [este año]."

Los informes de compañías como Websense, McAfee, Symantec y otros fabricantes de productos de seguridad reflejan la misma preocupación: los smartphones son un objetivo en constante y rápido crecimiento.

Los expertos dicen que el modelo de distribución abierta de la aplicación Android para Google la convierte en un blanco más atractivo para posibles atacantes. Con este modelo, los usuarios tienen la posibilidad de descargar aplicaciones desde una gran variedad de fuentes. Además de esto, "Android, en estos momentos, informa que hay 500.000 activaciones cada día," dice Runald. "Es una oportunidad demasiado buena para que los 'tipos malos' la dejen escapar."

A pesar de que, todavía, representa un porcentaje relativamente bajo con respecto al malware en general, la amenaza del malware en móviles está creciendo.

Por otra parte, la otra gran plataforma de smartphones es el Apple iOS, de código cerrado. Todas las aplicaciones iOS son enviadas a programadores y pasan por un proceso de revisión manual con restricciones basadas en ciertas reglas. Aunque normalmente se suele considerar una plataforma más segura que no permite que los usuarios descarguen aplicaciones no provenientes de la App Store de Apple, los usuarios pueden manipular y entrar en el dispositivo.

A pesar de que todavía representa un porcentaje relativamente bajo con respecto al malware en general, la amenaza del malware en móviles está creciendo. Mediante el malware, los atacantes pueden llevar a cabo ciertas acciones sin que el usuario lo sepa, como cargarle tarifas premium a su cuenta telefónica, enviar mensajes a su lista de contactos o, incluso, controlar de manera remota su dispositivo.

"El tipo de malware [móvil] ha cambiado bastante," dice Dirro. "Hace un

año, básicamente eran virus programados por niños en el patio del colegio." Según el reciente informe Threat Report de McAfee, los troyanos vía SMS de tarifa premium siguen siendo atractivos para los programadores de malware. Versiones nuevas de estos troyanos, como las familias Android/Wapaxy, Android/LoveTrp y Android/HippoSMS, a menudo suplantan a sus víctimas suscribiéndolas a determinados servicios y luego "astutamente borran todos los mensajes de confirmación de la suscripción, de modo que la víctima desconoce la actividad y el atacante gana más dinero," señala el informe.

Sin embargo, el spyware está adquiriendo popularidad rápidamente. Con este código, los atacantes tienen acceso al historial de llamadas, mensajes de texto, localización, historial del navegador, lista de contactos, email e, incluso, fotografías de la cámara. Android/PJApp envía mensajes SMS, pero también recopila esta información confidencial. Las llamadas telefónicas también pueden ser grabadas y enviadas al atacante. Android/NickiSpy.A y Android/GoldenEagle.A son dos ejemplos de spyware que pueden hacer esto con éxito.

Otra amenaza derivada de las aplicaciones tiene que ver con las apps vulnerables, aplicaciones que no son especialmente maliciosas pero cuyo software muestra vulnerabilidades que pueden ser explotadas para fines maliciosos. Dirro, el experto de McAfee, añade que este tipo de amenazas derivadas de las aplicaciones es una "forma inmediata de hacer dinero y, normalmente, [los atacantes] pueden quedarse fácilmente con ese dinero."

Otros expertos advierten que el problema del malware para móviles todavía no ha adquirido un tamaño lo suficientemente grande como para captar la atención absoluta de una empresa. Pete Lindstrom, Director de Investigación en la firma de investigación para la seguridad Spire Security, explica que es "mucho más fácil atacar una aplicación en un portátil" que en un smartphone. En primer lugar, los atacantes tienen que introducir una app maliciosa o malware para móviles en el dispositivo señalado como blanco y, luego, buscar la manera de esquivar las restricciones de seguridad de la plataforma móvil del teléfono.

"No se puede negar que existe una legítima preocupación de que estos

aparatos, a medida que crece su importancia, van a estar en el punto de mira de los programadores de malware," dice Lindstrom. "Es probable que su empresa tenga otros peligros mayores. Dicho esto, pienso que las empresas deberían tener cuidado con los smartphones."

Actualmente, la pérdida o robo de dispositivos sigue siendo una plaga para las empresas y constituye su principal amenaza, dice Lindstrom. Afortunadamente, las tecnologías de seguridad tienen la capacidad de localizar y limpiar el dispositivo en caso de que caiga en las manos equivocadas.

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

Runald, de Websense, pronostica una proliferación de la ingeniería social y las amenazas de geolocalización. "Los 'tipos malos' van a encontrar la manera de usar más técnicas de ingeniería social," explica. "Los servicios basados en la geolocalización están convirtiéndose en algo grande, así que ¿por qué no combinarlos con algo malicioso?"

"Estos son los días súper tempranos," añade Runald, quien predice que habrá varios miles de casos de malware para móviles, más del doble [este año]. "Los atacantes todavía están aprendiendo cómo usarlo, cómo difundirlo de la manera más efectiva y lo que pueden hacer con ello. No es, ni por asomo, tan avanzado como lo que va a llegar a ser." ■

El mercado de gestión de dispositivos móviles ofrece opciones para la seguridad de estos equipos

Averigua las opciones disponibles en cuanto a productos de gestión de dispositivos móviles y conoce cómo pueden contribuir a la seguridad móvil dentro de tu organización.

POR BILL HAYES

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

LOS FABRICANTES no paran de sacar al mercado nuevos y elegantes dispositivos móviles, y a los empleados les falta tiempo para hacerse con uno tras otro. Sin embargo, para los responsables de seguridad TI de las organizaciones, estos dispositivos presentan diversos y complejos problemas con respecto a la seguridad y la privacidad de los datos. Aquí es donde hace su entrada la tecnología de gestión de dispositivos móviles (MDM). Los productos MDM permiten a las organizaciones gestionar y proteger plataformas múltiples de dispositivos móviles corporativas y personales de los propios empleados. Básicamente, esto permite a los administradores de TI supervisar y controlar el uso de smartphones, tabletas y otros aparatos similares en el entorno corporativo.

"Las organizaciones necesitan una solución que facilite una integración segura de los dispositivos móviles con su infraestructura corporativa."

—JOHN MARSHALL
Presidente Ejecutivo, AirWatch, LLC

"Las organizaciones necesitan una solución que facilite una integración segura de los dispositivos móviles con su infraestructura corporativa, como los servicios de directorio, email, Wi-Fi, VPN," dice John Marshall, Presidente Ejecutivo de AirWatch LLC., un proveedor de MDM con sede en Atlanta.

Ojas Rege, vicepresidente de productos y marketing de MobileIron Inc.,

una empresa de Mountain View, California, dedicada a la gestión de dispositivos móviles, dice que los productos MDM están diseñados para dar respuesta a cinco retos clave aparejados con la gestión de la seguridad en diversos dispositivos móviles orientados al consumo.

Según Rege, los productos MDM posibilitan la gestión de activos para mantener un seguimiento de los inventarios y la propiedad de smartphones y tabletas; gestión de arquitecturas para controlar las configuraciones de los dispositivos móviles de cara a la conectividad, privacidad, seguridad y aplicaciones empresariales; protección de datos, tanto para la información estática en el aparato como para la información en movimiento, desde y hacia el dispositivo; gestión de aplicaciones para organizaciones, lo que, a menudo, permite a la empresa ofrecer su propia "app store" para distribuir aplicaciones móviles y garantizar la seguridad de los datos de las aplicaciones; y, por último, solución de problemas y servicio de asistencia como soporte para el usuario.

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

CUÁNDO USAR MDM, FACTORES DE TENSIÓN

Según Marshall, los productos MDM son los más idóneos para las organizaciones de tamaño mediano y grande que buscan permitir el acceso de los dispositivos corporativos o personales de los empleados a los recursos internos de la empresa, bien sean email, VPNs, Wi-Fi, aplicaciones móviles, o aplicaciones de empresa como Microsoft SharePoint, ERP u otros sistemas propios.

Rege dice que la MDM funciona bien cuando la organización permite o sostiene sólo un tipo de dispositivo, como el BlackBerry, pero quiere permitir en el futuro el uso de otros dispositivos móviles y necesita proteger la información corporativa que llegue a esas plataformas móviles adicionales. O, también, si la organización está realizando la migración desde email móvil a las aplicaciones móviles y necesita proporcionar mecanismos para la distribución, descubrimiento por parte del usuario final o seguridad de los datos de las aplicaciones.

"Un factor de tensión para muchas empresas es la presión de los emplea-

dos para aplicar el BYOD (del inglés *bring your own device* o 'trae tu propio dispositivo')," dice Lisa Pittenger, directora de productos para la movilidad en la empresa, de la firma de productos de seguridad McAfee Inc., radicada en Santa Clara, California.

"A medida que crece el número de dispositivos personales con acceso a información corporativa, sigue habiendo una cierta tensión con respecto a la gobernanza y las cuestiones relacionadas con la privacidad en el caso de que un empleado dejase [la empresa] y [hubiese que plantearse] limpiar (*wipe*) el dispositivo," dice Pittenger. "Es importante que la empresa tenga una política de BYOD y unas normas claras sobre lo que ocurriría con la información si se da esa situación."

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

Según Kevin Johnson, un instructor de SANS y consultor en materia de seguridad con la firma Secure Ideas, con sede en Jacksonville, Florida, otros puntos de tensión relacionados con la MDM incluyen el diseño de las políticas y la obtención de autorización de las fuentes apropiadas para restringir la funcionalidad de las prestaciones del dispositivo móvil elegidas. Johnson explica también que la decisión sobre qué dispositivos están suscritos a la MDM, debido a la continua rotación de aparatos móviles, puede suponer otro quebradero de cabeza.

Para tener éxito, los productos MDM deben soportar al menos tres o más sistemas operativos para dispositivos móviles.

Diseñar una nueva clase de políticas de seguridad y privacidad para dispositivos móviles puede suponer un desafío para los empleados porque la MDM es fundamentalmente diferente de las normas que rigen la tecnología, comportamiento y requisitos de uso de las computadoras y portátiles, ámbitos en los que, a veces, se sacrifica la experiencia del usuario a cambio de mejorar la seguridad o la gestión remota, dice Rege. La MDM debería permitir elegir dispositivos y aplicaciones sin interferir con el funcionamiento del dispositivo ni con la experiencia del usuario, añade.

Para tener éxito, continúa Rege, los productos MDM deben soportar, al

menos, tres o más sistemas operativos para dispositivos móviles, como iOS o Android, incluir configuraciones de seguridad de inicio y avanzadas, así como un inline proxy para proteger la información en movimiento.

Rege considera que entre las prestaciones que no pueden faltar están la integración estrecha con el Directorio Activo y el Protocolo Ligero de Acceso a Directorios (LDAP), así como otros sistemas de gestión de la identidad (IM) y de seguridad, todo ello combinado con la gestión de aplicaciones móviles de un extremo a otro.

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

Según Marshall, es importante tener en cuenta si un producto es capaz de una agrupación avanzada o de multiusuarios que permita la autonomía entre regiones o cuentas de resultados, pero que ofrezca, a la vez, cierto grado de control centralizado y gestión de activos.

"Observamos muchas soluciones ad hoc o decisiones distribuidas de grandes multinacionales, principalmente debido a una sensación de urgencia para ponerse en marcha rápidamente," dice Marshall.

Johnson dice que los productos MDM deben ser capaces de agrupar a los usuarios y a los dispositivos en configuraciones específicas. También recalca la necesidad de contar con capacidades sólidas de elaboración de informes a fin de que las organizaciones puedan ver qué está ocurriendo con los dispositivos y las configuraciones.

La existencia de múltiples partes interesadas también puede ser un punto de tensión, afirma Vizay Kotikalapudi, gerente principal de movilidad y gestión de endpoints de Symantec Corp.

"Todavía no está claro quién gestiona la movilidad en las organizaciones, y hay múltiples equipos con intereses en la movilidad," dice Kotikalapudi. "Por ejemplo, el equipo de mensajería los tiene para el email móvil, el de infraestructuras para las aplicaciones móviles, el de seguridad para cuestiones de seguridad, el de operaciones/servicio de asistencia para las tareas del día a día."

"La fricción dentro de la organización está garantizada a medida que las necesidades de todos estos equipos evolucionan," dice Kotikalapudi. "Contar con objetivos claros, compartidos y con la complicidad del usuario contribuirá a aliviar este tipo de conflictos."

AGENTES DEL CAMBIO A CORTO PLAZO EN LA MDM

Según el Cuadrante Mágico de Gartner del mes de abril de 2011 para el mercado de gestión de dispositivos móviles, entre los líderes actuales del mercado se encuentran AirWatch, Good Technology, MobileIron y Sybase. Sin embargo, Gartner afirma que no hay un solo fabricante que ofrezca un producto integral para la gestión de aplicaciones, servicios, políticas, dispositivos y seguridad. Esto significa que es muy probable que los paquetes de prestaciones de los productos actuales de MDM seguirán expandiéndose aún más en un esfuerzo por cubrir todas estas lagunas.

Sin embargo, hay otros agentes que están impulsando el crecimiento y la evolución del mercado de productos MDM. Pittenger, de McAfee, dice que el crecimiento del malware para dispositivos móviles ha incrementando la importancia de crear un sistema integral de salvaguardas para las plataformas móviles antes de permitirles acceso a las redes corporativas y los recursos allí almacenados.

"La distribución de aplicaciones, su cumplimiento con la normativa establecida y la seguridad serán cada vez más importantes durante los próximos meses," dice Marshall. "Para ser completamente productivos, los trabajadores con movilidad no sólo esperan tener los aparatos de última generación, sino también un paquete de aplicaciones complementarias. Además, las aplicaciones para móviles se han convertido en una iniciativa estratégica para muchas organizaciones, creando un factor de diferencia competitiva en sus mercados."

"Los requisitos de seguridad/cumplimiento en este nuevo contexto van a ser todavía más complejos," señala Kotikalapudi. "Tener un enfoque centrado en la información frente al enfoque basado en el dispositivo es lo que va a dar un mejor resultado a largo plazo." ■

Emergen las opciones de seguridad SaaS como defensa ante los riesgos de seguridad de los dispositivos móviles

Los servicios de seguridad móvil basados en la nube pueden ayudar a defenderse contra el malware y a proteger la información sensible. **POR MARCIA SAVAGE**

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

A MEDIDA que las empresas tratan denodadamente de obtener cierta semblanza de control sobre todos los smartphones y tabletas que sus empleados traen al trabajo, las opciones de protección contra los riesgos de seguridad de los dispositivos móviles se expanden y entran en el terreno de la seguridad SaaS.

IBM anunció el diciembre pasado la introducción de un servicio basado en la nube que, según la empresa, ayudará a las organizaciones a mitigar los riesgos generados por la posibilidad que tienen los dispositivos móviles personales de acceder a información corporativa de carácter sensible. Este nuevo servicio de IBM está diseñado para poner en práctica políticas corporativas para un abanico de dispositivos móviles, ayudar a localizar dispositivos perdidos, salvaguardar datos en caso de pérdida o robo del aparato, proteger contra el malware y hacer seguimiento a la actividad de los usuarios.

Asimismo, el pasado otoño, Symantec Corp. anunció que tiene previsto ofrecer un servicio en la nube para proveedores de comunicaciones que les posibilita ofrecer servicios de seguridad a sus usuarios de dispositivos móviles. El servicio permite a las compañías controlar el acceso desde plataforma móviles a sitios Web y comprobar que las descargas desde la Red están libres de malware.

Mientras tanto, Zscaler Inc., un proveedor de SaaS para seguridad de la Web y del correo electrónico lleva algún tiempo probando su servicio para la protección de dispositivos móviles con alrededor de una docena de clientes

corporativos y tiene previsto empezar a comercializarlo el primer trimestre del año próximo.

El mercado de SaaS para la seguridad del contenido de los dispositivos móviles sólo está empezando a nacer aunque ya hay varias firmas desarrollando servicios que estarán disponibles en el mercado este mismo año, dice Rick Holland, analista principal de Forrester Research.

Hay cierto nerviosismo acerca de los riesgos que los dispositivos móviles presentan para la seguridad, pero la realidad es que los ataques contra las plataformas móviles son inevitables, dice Holland. “Estas soluciones de protección de contenidos nos van a ayudar con eso,” añade.

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

El modelo de seguridad móvil basado en la nube puede proporcionar una mejor experiencia al usuario porque reduce los problemas de latencia, dice Holland. Con un producto centralizado de seguridad de contenidos tradicional, la protección del usuario de dispositivos móviles que trabaja en una ubicación remota puede exigir reconducir el tráfico a la sede corporativa. Por el contrario, con el modelo basado en la nube, el usuario remoto puede estar conectado al nodo de nube más cercano, añade.

Sea cual sea el sistema de seguridad móvil basada en la nube, las compañías deberían prestar atención a cuáles son las plataformas cubiertas, advierte Diana Kelley, socia de SecurityCurve, una firma de consultoría radicada en Amherst, New Hampshire. “La no cobertura de todas las plataformas es particularmente problemático debido a la popularidad de ‘Droid e iOS’,” escribió en un email.

Zscaler (Sunnyvale, California) actualmente centra sus esfuerzos en la protección de dispositivos Apple para la empresa, dice Amit Sinha, su director tecnológico. “Los mecanismos de redireccionamiento del tráfico en Android y otros dispositivos son todavía un poco prematuros,” dice. “A medida que vayan reforzando su base Web y empiecen a soportar las redes estándar, como los túneles VPN, de forma confiable podremos extender esa protección a todos estos dispositivos.”

En última instancia, el enfoque basado en la nube de Zscaler hace abstracción de los dispositivos, dice Sinha. “No nos importa si el tráfico llega de un portátil, de una tableta Android o de un iPhone. Somos la puerta de acceso

al tráfico," dice.

Si bien el sistema centralizado a partir de una infraestructura física se encuentra con el problema del retorno (backhauling), el modelo tradicional basado en agentes ubicados en un endpoint también tiene problemas en los contextos móviles porque se hace necesario actualizar los agentes locales, dice Sinha. Zscaler no tiene clientes y simplemente se apoya en el estándar IPSec del cliente VPN de Apple, explica.

Otro proveedor de SaaS de seguridad, Proofpoint, Inc., no ofrece servicios de gestión de dispositivos móviles u otras aplicaciones específicas de seguridad móvil, pero ha optimizado sus servicios a plataformas móviles con base en la nube.

Proofpoint, también de Sunnyvale, California, una firma especializada en comunicaciones seguras y archivado de emails, añade la posibilidad de que los usuarios puedan desencriptar fácilmente mensajes en sus dispositivos móviles. La compañía también ha expandido su servicio de archivado para dejar que los usuarios móviles puedan acceder al correo de años múltiples en lugar de las últimas tres o cuatro semanas que es la norma en este tipo de dispositivos, dice Andres Kohn, vicepresidente de tecnología de Proofpoint.

De cara al futuro, Kelley, de SecurityCurve, espera que la tecnología de control y seguridad de dispositivos móviles madurará hasta llegar a proporcionar un control y unos mecanismos de aplicación de las políticas más sólidos. Al mismo tiempo, espera que las compañías estudien más de cerca otras formas de controlar la información sensible, quizás no permitiendo que se copie en ningún lugar o dejando que solamente sea visualizable a través de una infraestructura virtual de computadora .

"En algún momento, creo que las empresas van a tener que agarrar el toro por los cuernos en lo que se refiere a la replicación de información sensible," dice. "Sé que mucha gente no está de acuerdo con esto porque es muy restrictivo, pero creo que es la mejor estrategia para la información altamente sensible." ■

SAAS

¿Preocupado por la seguridad de las tabletas? Algunos lo están; otros, no tanto

Las tabletas perdidas o robadas pueden contener información corporativa confidencial o proporcionar a los ladrones la oportunidad de acceder a las cuentas corporativas. ¿Pero están justificados los temores sobre la seguridad de las tabletas? **POR RON CONDON**

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

LA TABLETA se está convirtiendo en uno de los compañeros electrónicos favoritos de los usuarios, y eso es precisamente lo que pone en guardia a algunos responsables de TI que ven que las tablas proliferan sin ningún control y se usan para acceder tanto a las aplicaciones corporativas como a aplicaciones descargadas de Internet sin ninguna inspección o test previo.

Las tabletas perdidas o robadas pueden contener información corporativa confidencial o proporcionar a los ladrones la oportunidad de acceder a las cuentas corporativas. ¿Pero están justificados los temores sobre la seguridad de las tabletas?

LAS POLÍTICAS DE SEGURIDAD ESTABLECIDAS DEBERÍAN SER SUFICIENTES

Según Jamie Marshall, director de soluciones TI en Equanet, una firma de integración de sistemas con sede en Bury, Reino Unido, y filial de Dixons Retail, gran parte de la ansiedad que rodea a las tabletas está injustificada. "Existe la percepción de que, al ser dispositivos tan usables y que están siempre encendidos, son por naturaleza inseguros. Pero una vez que la gente entiende cómo funciona la seguridad de las tabletas dejan de considerarla un problema," dice Marshall. Este ejecutivo alega que, por ejemplo, la encriptación que lleva incorporado el iPad lo hace muy seguro. "Como empresa, todo lo que necesitas es poner en práctica una política de códigos de acceso

fuertes para los usuarios. Si se pierde el dispositivo, nadie puede entrar en él y se puede llevar a cabo una limpieza remota del mismo."

Sin embargo, aplicar estas políticas para las tabletas puede resultar complicado porque las distintas plataformas existentes operan de forma diferente. Pero la tarea puede facilitarse con el empleo de un sistema de gestión de dispositivos móviles (MDM), el cual permite a los administradores establecer normas de funcionamiento y aplicarlas en múltiples plataformas. Equanet usa AirWatch para su uso personal; otros proveedores de sistemas MDM son Good Technology, MobileIron y Sybase.

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

Marshall dice que si las empresas suministran dispositivos a los empleados, tienen derecho a poner en práctica sus políticas de protección de la información, pero si los usuarios están autorizados a conectar sus propios aparatos, entonces mantener el control puede ser más complicado.

Sin embargo, incluso cuando el usuario, y no la empresa, es el propietario del dispositivo, Marshall sigue aconsejando que dicho equipo quede bajo control del sistema MDM para poder, así, exigir el establecimiento de códigos de acceso fuertes. "También deberías hacer saber a los usuarios que si utilizan el dispositivo para asuntos de trabajo y, posteriormente, deciden dejar la empresa, tienes la capacidad para limpiarlo. Eso hay que hacerlo a través de un acuerdo," dice.

ASPECTOS PREOCUPANTES DE LAS TABLETAS

Algunas personas son menos optimistas respecto a la amenaza que suponen las tabletas. "Las tabletas, como tecnología, todavía son relativamente inmaduras," dice Phil Robinson, directivo de la consultora londinense Digital Assurance. "No tienen tantos parches ni actualizaciones y el ciclo de actualización no es tan frecuente como en Windows. Además, el usuario tiene unos grandes niveles de privilegio sobre el dispositivo."

Rob Newburn, director de seguridad de la información en Trustmarque Solutions, una firma de York, concuerda con Robinson. "Muchos de estos dispositivos no fueron diseñados para los negocios," dice. Por un lado, la amenaza de los virus móviles hacia las tabletas es todavía pequeña, añade;

las principales amenazas para las tabletas son la filtración de datos y la pérdida de productividad.

Ian Kilpatrick, presidente del directorio de Wick Hill Group, una distribuidora de productos de seguridad radicada en Woking, compara la situación actual con la que se vivió hace 10 años con las computadoras portátiles conectadas a distancia. "Al igual que cuando llegaron las primeras portátiles PC, [ahora] la aplicación es la que dirige la operación, y luego es la seguridad la que sigue detrás tratando de arreglar las cosas," dice. "Algunas compañías han implementado un poco de seguridad pero no tienen una política coordinada, y por lo tanto, son incapaces de gestionar el problema en su totalidad. Permiten a sus empleados el acceso a la red para poder leer su email y luego los empleados utilizan ese acceso para entrar en otros sistemas."

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

TRAZAR UN RUMBO PARA LA PROTECCIÓN DE LAS TABLETAS

Todo el mundo parece estar de acuerdo en que las tabletas —en todas sus variantes—estan aquí para quedarse, y eventualmente, tendrán que tener mantenimiento. Lo peor que puede hacer una compañía es ignorar esta tendencia porque eso sólo servirá para estimular la entrada de tabletas por la puerta de atrás. Esto es lo que dice Ray Stanton, vicepresidente de servicios profesionales en la empresa londinense BT Global Services. "Si la política consiste en permitir el uso de tabletas, entonces hay que introducir las mis-

Masificación del consumo de la tecnología

Según una investigación realizada por Equanet en octubre, la Masificación del consumo de la tecnología es una realidad indiscutible en nuestras vidas. Tras entrevistar a 1.287 gerentes de TI de empresas pequeñas y medianas, esta firma descubrió que en el 18% de las empresas ya se emplean tabletas en el centro de trabajo y que el 71% de los dispositivos en uso son propiedad de los propios trabajadores.

mas normas de seguridad y exigir su cumplimiento de la misma forma que si se tratara de una computadora portátil," dice. "Es irrelevante si se trata de tu propio dispositivo. Si los usuarios tienen acceso a la información corporativa, las reglas a aplicar son las de la empresa, independientemente del equipo con el que han accedido a ella."

Algunas empresas importantes están logrando combinar el equilibrio delicado entre libertad de uso y control estrecho sobre la información. Por ejemplo, la gigante de las redes Cisco introdujo una política de 'trae tu propio dispositivo' (BYOD) en 2009 y, según el CTO de la empresa en el Reino Unido, Ian Foddering, la respuesta ha sido entusiasmada en todo el mundo.

Está claro que el antiguo enfoque para los dispositivos móviles, con bloqueo y fabricación estándar, está perdiendo vigencia a pasos agigantados

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

Más de 17.000 empleados de Cisco utilizan sus smartphones para su trabajo y la compañía está viendo cómo, cada mes, aumenta en 400 el número de nuevos iPads utilizados por empleados que prefieren usar su propio dispositivo en vez de el equipo portátil que les ofrece la empresa. Los usuarios que registran sus aparatos tienen que descargar un cliente VPN para conectarse con la información corporativa y firmar un acuerdo que permite a Cisco limpiar su dispositivo de forma remota en caso de pérdida o riesgo de uso indebido.

Es más, los usuarios tienen que darse apoyo a sí mismos, de modo que todos los problemas técnicos se tratan y solucionan entre ellos a través de su participación en un foro en linea. "Debido a la autoayuda, hemos visto un descenso del 20% en el número de casos tratados por el servicio de asistencia," dice Foddering.

Está claro que el enfoque antiguo para los dispositivos móviles, con bloqueo y fabricación estándar, está perdiendo vigencia a pasos agigantados. Estamos ante una industria en movimiento rápido; el lanzamiento paneuropeo del iPad se produjo sólo hace dos años. Tanto Apple como Google están trabajando para hacer que sus productos sean más fáciles de manejar

y proteger, y los fabricantes de productos tecnológicos aceleran esfuerzos para ofrecer fórmulas para la gestión de los nuevos dispositivos.

Mientras tanto, los encargados de la seguridad hacen lo que pueden. "Estos aparatos han aparecido en el mercado muy rápidamente y con un relativo desdén por la seguridad. Ahora existe el riesgo de que los usuarios trasladen esa despreocupación a los centros de trabajo. Tenemos que llevar a cabo un proceso educativo con los usuarios," dice Newburn, de Trustmarque Solutions.

"Es una decisión básica de seguridad. Si los riesgos pesan más que los beneficios para el negocio, no permitirlo. Si los beneficios superan a los riesgos y puedes mitigar éstos hasta un nivel aceptable, entonces adelante y abre los brazos a las tabletas." ■

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

Seguridad 'trae tu propio dispositivo': ¿Qué opina India S.A.?

Conoce el enfoque de los profesionales indios hacia la seguridad BYOD. **POR VARUN HARAN**

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

UNA ENCUESTA reciente de ISACA sobre la proliferación de la cultura BYOD ('trae tu propio dispositivo') en los centros de trabajo de la India puso de manifiesto cuestiones importantes relacionadas con la seguridad. La encuesta establece que la mayoría de los incidentes de seguridad surgen del uso que hacen los empleados de los activos tecnológicos, bien sea por el uso de aparatos personales en la red de la compañía o por usar equipos de la empresa para disfrute personal. Los expertos creen que el abaratamiento de estos dispositivos, repletos de prestaciones, está abriendo una caja de Pandora en materia de seguridad.

Cada industria vertical de la India tiene que luchar contra sus propios demonios relacionados con BYOD. Mientras que las empresas de los sectores bancario y financiero y TI/ITES están más preocupadas por la privacidad de sus clientes, otros sectores tienen las manos llenas con la protección de su información restringida. Sin embargo, aspectos como el robo de datos, la intrusión en las redes y los daños económicos generados por este nuevo vector son la prioridad en las agendas de trabajo de todos los responsables de seguridad.

LA PESADILLA DE LA SEGURIDAD BYOD

Cada vertical tiene su propia estrategia contra el problema de la seguridad BYOD. Aunque la integración permitida dependerá del perfil de riesgo específico de la organización, expertos a lo largo y ancho de la industria se muestran de acuerdo en que, si bien estos dispositivos pueden ser de gran ayuda para la productividad, su seguridad puede constituir una verdadera pesadilla.

Raja Vijay Kumar, vicepresidente y responsable global de seguridad de la información de Genpact, no es una excepción. Como persona responsable de la seguridad de los 40.000 empleados—la mayor parte de ellos con edades comprendidas entre los 25 y 30 años—de esta empresa contratista de servicios empresariales, la seguridad BYOD supone, sin lugar a dudas, un verdadero reto. Las cuestiones a resolver abarcan desde la responsabilidad legal hasta la necesidad de proteger las áreas más confidenciales de la empresa.

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

Asimismo, Genpact está examinando el caso de negocio para los empleados que trabajan desde cualquier lugar empleando sus propios dispositivos. Uno de los retos más singulares a los que se enfrenta Kumar es el de hacer que los clientes se impliquen en estas iniciativas, dada la naturaleza tan sensible del negocio de Genpact y de los marcos regulatorios.

Cuanto mayor sea el riesgo, menor es la probabilidad de que la dirección autorice tecnologías que pudieran exponer la organización a un ataque.

Para Satish Das, director ejecutivo de seguridad y vicepresidente de ERM (Gestión de Riesgos Empresariales) en Cognizant Technologies, una de las empresas líderes del sector de TI y servicios gestionados, no se trata tanto del 'cómo', sino del 'cuándo'. Dicho esto, Das cree que el hecho de que los dispositivos no sean propiedad de la organización abre la posibilidad a cuestiones de responsabilidad legal y otros asuntos relacionados con la privacidad. Los empleados también son ahora más exigentes y conocen mejor sus derechos.

Según Deepak Rout, director de seguridad de la información (CISO, según sus siglas en inglés) de Uninor, la productividad que aportan estos dispositivos es incuestionable. Pero la organización tiene que mantener la cautela respecto a la información que permite que llegue a estos equipos. Según Rout, en última instancia todo depende del tipo de dispositivo y del uso que se le dé.

La mayoría de las organizaciones necesitan contar con un servicio de email disponible en todo momento, y algunas incluso proporcionan aplicaciones ERP/CRM para dispositivos inteligentes. Con todas las aplicaciones,

siempre y cuando no se pueda acceder con el dispositivo a información sensible—o dicha información sensible pueda ser controlada—el problema se centra, simplemente, en la integración de otro punto de entrada a la red.

Las tecnologías emergentes hoy en día permiten un control preciso y granular de la seguridad BYOD, dice Rout. Por ejemplo, Microsoft Exchange Server 10 SP2 ahora proporciona la posibilidad de enviar documentos adjuntos en formato 'read only', una funcionalidad que ni siquiera permite, todavía, la plataforma BlackBerry. En el caso de que un dispositivo se convierta en punto de entrada para un ataque contra la organización, siempre y cuando se haya establecido un perímetro sólido y bien definido, los ataques pueden ser detenidos con facilidad.

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

ESCENARIO ACTUAL

Así pues, ¿qué están haciendo las grandes lumbreras del sector para controlar las amenazas de seguridad derivadas del BYOD? Las respuestas oscilan entre la prohibición total y absoluta hasta la adopción de filosofías más avanzadas.

Según Kumar, de Genpact, "aparte de los smartphones, en estos momentos Genpact no permite el uso de otros dispositivos para cuestiones relacionadas con el negocio." Tambien dice que aunque Genpact ha abierto el camino a los smartphones, se han instaurado controles adecuados para minimizar la exposición.

Kumar explica que la iniciativa de "trabajar con su propio dispositivo" no puede ir para adelante sin el consentimiento de los clientes; además, es preciso que exista una transparencia total, según la cual Kumar y su equipo comparten el diseño y los controles de la seguridad BYOD para ganarse la confianza completa de sus clientes. Con tecnología VDI y de cliente ligero espera que, en un futuro, los empleados puedan trabajar desde su hogar sin poner en peligro la seguridad de la organización. Sin embargo, añade que él va a esperar a que la tecnología de seguridad BYOD madure antes de tratar de ampliarla al trabajo desde el hogar.

Das, de Cognizant, se muestra mucho más cauto, ya que cree que el nivel

de seguridad que exigen estos dispositivos todavía no está totalmente instalado. Al igual que otros, Das está de acuerdo en que la decisión de permitir un política de BYOD está determinada por el perfil de riesgo de la organización. Cuanto mayor sea el riesgo, menor es la probabilidad de que la dirección autorice tecnologías que pudieran exponer la organización a un ataque.

El CISO de Essar Group, Manish Dave, dice que su organización no autoriza los dispositivos inteligentes en la red corporativa a fin de preservar la seguridad de los dispositivos personales. Aparte de las plataformas protegidas, como BlackBerry, donde es posible su regulación, Dave no cree que sería inteligente dejar que estos dispositivos móviles tengan acceso a la red corporativa, ya que no hay forma alguna de garantizar un cumplimiento absoluto de las políticas de seguridad de la empresa.

Por lo tanto, en la actualidad, en Essar sólo se permiten dispositivos BlackBerry. Para garantizar una robusta seguridad BYOD, la organización ejerce un control granular sobre estos dispositivos, inhabilitando opciones como la capacidad para guardar documentos adjuntos. Otros aparatos de uso personal, como los portátiles, no se permiten en las redes corporativas a menos que se adhieran a la política corporativa de protección de la información.

Dave dice que, aunque los dispositivos más recientes, como el iPad o el iPhone 4, vienen de fábrica con mecanismos de control más estrictos, todavía hay un largo camino que recorrer antes que la seguridad BYOD quede perfectamente integrada en el resto de la infraestructuras TI. Según este experto, Essar está en estos momentos examinando la posibilidad de adaptar la solución Afaria de Sybase como sistema de gestión integral de dispositivos móviles.

Dentro de la estrategia de seguridad hacia los BYOD de Uninor, Rout no permite el acceso a información sensible cuando la petición de acceso llega desde un punto remoto. “Como mejor práctica, no se debería permitir el acceso remoto a ningún empleado. El acceso sin restricciones debe realizarse sólo con el hardware adquirido y mantenido por la empresa, donde el entorno puede ser controlado y es posible exigir responsabilidades por su utilización,” concluye Rout. ■

SOBRE LOS AUTORES

Hillary O'Rourke es colaboradora de SearchSecurity.com

Bill Hayes es escritor freelance y consultor. Vive en Nebraska.

Ron Condon es director en el Reino Unido de la oficina de Security Media Group, filial de TechTarget.

Varun Haran colabora con Search Security.in y SearchDataCenter.in. Es Licenciado en Ciencias Económicas y tiene un Diploma de Postgrado en Periodismo por ACJ, Chennai.

AMENAZAS

MDM

SAAS

TABLETAS

BYOD

TechTarget

Esta *Guía Tecnológica sobre Seguridad Móvil* es una publicación electrónica de SearchSecurity.com

Michael S. Mimoso
Director Editorial

Eric Parizo
Editor Principal Web

Robert Westervelt
Director de Noticias

Marcia Savage
Editora Web

Ron Condon
Director Oficina Reino Unido

Kara Gattine
Jefa de Redacción Senior

Doug Olender
Vicepresidente/Editor Jefe del Grupo
dolender@techtarget.com

Peter Larkin
Editor Jefe Asociado
plarkin@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

Acerca de TechTarget: TechTarget publica contenidos para los profesionales de las tecnologías de la información. Más de 100 sitios web especializados permiten el acceso rápido a un gran archivo de noticias, consejos y análisis sobre tecnologías, productos y procesos esenciales para nuestro trabajo. Nuestros eventos virtuales y en vivo te ofrecen un acceso directo a comentarios y consejos de expertos independientes. Acércate a nuestra comunidad social IT Knowledge para obtener consejos y compartir soluciones con otros profesionales y expertos.