Informe Anual de Seguridad de Cisco 2011

DESTACAMOS LAS AMENAZAS Y TENDENCIAS EN SEGURIDAD A NIVEL MUNDIAL

cisco

El *Informe Anual de Seguridad de Cisco*® brinda una visión general de la inteligencia de seguridad combinada de toda la organización de Cisco. El informe comprende información sobre amenazas y tendencias recopilada entre enero y noviembre de 2011. También ofrece una instantánea del estado de la seguridad durante dicho período y presta particular atención a las principales tendencias en seguridad que se anticipan para 2012.

PRIMERA PARTE

3 Le damos la bienvenida al Mundo Conectado

5 **Sus futuros empleados:** Equipados con dispositivos y no muy preocupados por la seguridad

8 **Medios sociales:** Hoy, una herramienta de productividad

10 **Acceso remoto y estrategia BYOD:** Empresas que trabajan para encontrar puntos en común con los empleados

16 La influencia de los dispositivos móviles, los servicios en la nube y los medios sociales en la política de seguridad de la empresa

SEGUNDA PARTE

22 **Panorama de amenazas cibernéticas para 2012:** El factor del ciberactivismo pirata

23 **Tendencias geopolíticas:** Los medios sociales ejercen el poder de “reunión”

24 Anuncio de los ganadores de 2011 de Cisco Cybercrime Showcase

26 Matriz de Cisco del Retorno de la inversión de la ciberdelincuencia (CROI)

28 Análisis de vulnerabilidades y amenazas de 2011

29 **Actualización sobre el correo no deseado a nivel mundial:** Disminución radical del volumen de correo no deseado

31 El Índice Cisco Global ARMS Race

32 **Internet:** ¿Una necesidad humana fundamental?

35 Inteligencia sobre seguridad de Cisco

PARTE

1

Le damos la bienvenida al Mundo Conectado

Imagine la oficina de los años sesenta de la agencia de publicidad de ficción del programa de televisión estadounidense “Mad Men”: Si reparamos en la tecnología, veremos que los únicos equipos que los empleados podían utilizar para aumentar su productividad eran las máquinas de escribir y los teléfonos (cuyo usuarios principales solían ser las secretarias). Los empleados participaban en, quizá, una o dos reuniones por día; el trabajo comenzaba cuando llegaban a la oficina y terminaba cuando se iban a su casa.

Hoy en día, los empleados logran realizar más tareas durante el desayuno o el viaje al trabajo que lo que lograban sus predecesores en los años sesenta en una jornada completa. Gracias a la amplia gama de innovaciones tecnológicas que llegan al lugar de trabajo, desde tablets hasta redes sociales y sistemas de videoconferencia como telepresencia, los empleados pueden trabajar casi desde cualquier lugar y en cualquier momento en que necesiten hacerlo, con la condición de que dispongan de la tecnología adecuada de conectividad y, lo que es más importante, de seguridad. En efecto, una de las diferencias más notables entre el lugar de trabajo moderno y el de los sesenta es la ausencia de personas reales: Cada vez es menos necesario ir en persona a la oficina.

Junto con la avalancha de innovaciones tecnológicas, también se ha producido un cambio de actitud. Hoy en día, los empleados están tan acostumbrados a las ventajas de productividad y la facilidad de uso de sus dispositivos, las redes sociales y las aplicaciones web que no ven razones para no usar todas esas herramientas, tanto en el ámbito laboral como en la diversión. Prácticamente no existen los límites entre la oficina y el hogar: Estos empleados hablan con sus supervisores por Facebook, controlan sus mensajes de correo electrónico laborales en los iPads de Apple después de ver una película con sus hijos y convierten sus propios smartphones en mini estaciones de trabajo.

No sorprende, pues, que muchas empresas se pregunten por el impacto que tienen la innovación tecnológica y los hábitos laborales flexibles sobre la seguridad de la información empresarial, y a veces adopten medidas tan drásticas como prohibir los dispositivos o restringir el acceso a servicios web que los empleados dicen necesitar (lo que es cierto en la mayoría de los casos). No obstante, las organizaciones que no ofrezcan a sus empleados la suficiente flexibilidad (por ejemplo, los limitan a usar un determinado smartphone de la compañía), en poco tiempo verán que no pueden atraer a empleados talentosos ni mantener su capacidad de innovación.

En una investigación realizada para el estudio de *Cisco Connected World Technology Report [Informe de Tecnología del Mundo Conectado de Cisco]* (www.cisco.com/en/US/netsol/ns1120/index.html) se demuestran los cambios de las actitudes hacia el trabajo, la tecnología y la seguridad entre estudiantes universitarios y jóvenes profesionales de todo el mundo, que impulsan las nuevas olas de cambio en la empresa. (Los empleados de todas las edades han contribuido con el aumento en la adopción de dispositivos de consumo en el lugar de trabajo y el acceso a la información en cualquier momento y lugar; sin embargo, los empleados más jóvenes y los recién egresados están aumentando de forma radical el ritmo del cambio.) En la edición de este año del Informe Anual de Seguridad de Cisco se destacan numerosos hallazgos clave de esta investigación, que explora el impacto en las empresas y sugiere estrategias para fomentar la innovación.

Por ejemplo, la mayoría de los estudiantes universitarios encuestados a nivel mundial (81%) consideran que deben poder elegir los dispositivos que necesitan para trabajar, en cuyo caso los empleadores deberían pagar esos dispositivos o permitirles llevar sus propios dispositivos personales al trabajo. Por otra parte, casi las tres cuartas partes de los estudiantes encuestados consideran que deben poder usar los dispositivos tanto con fines profesionales como personales. La multiplicidad de dispositivos es cada vez más común: El 77% de los empleados encuestados a nivel mundial utilizan varios dispositivos, como una laptop y un smartphone, o varios teléfonos y computadoras. (Consulte “Sus futuros empleados: Equipados con dispositivos y no muy preocupados por la seguridad” en la página 5.)

Un enfoque equilibrado y flexible de la seguridad

Las tendencias tales como la llegada de los dispositivos de consumo al lugar de trabajo exigirán soluciones más flexibles y creativas al personal de TI para mantener la seguridad y habilitar el acceso a tecnologías de colaboración. Ante el deseo de los empleados de llevar los dispositivos que usan en su casa al lugar de trabajo, es preciso que las empresas adopten una visión “BYOD” (sigla en inglés de “trae tu propio dispositivo”); es decir que deberán proteger la red y los datos independientemente del método de acceso a la información que utilicen los empleados. (Consulte “Acceso remoto y estrategia BYOD: Empresas que trabajan para encontrar puntos en común con los empleados” en la página 10.)

"Hoy, los departamentos de TI deben aceptar el caos proveniente de un entorno BYOD", explicó Nasrin Rezai, director senior de arquitectura de seguridad de Cisco y director de seguridad del Grupo Empresarial de Colaboración. "Esto no supone aceptar altos niveles de riesgo, sino estar dispuesto a administrar algunos riesgos para atraer talentos y ofrecer innovación. Se trata de ingresar en un mundo en el que el departamento de TI no podrá administrar todos los recursos tecnológicos".

La disposición a lograr el equilibrio entre riesgos y beneficios es la característica distintiva de la nueva posición del departamento de TI frente a la seguridad. En lugar de prohibir lisa y llanamente los dispositivos o el acceso a medios sociales, es imprescindible que las empresas concedan flexibilidad a cambio de controles que los empleados aceptan respetar. Por ejemplo, el equipo de TI podría decir: "Puedes utilizar tu smartphone personal para leer y responder a los mensajes de la compañía, pero tenemos que administrar ese recurso. Y si pierdes ese teléfono, vamos a tener que borrar los datos a distancia, así como tus aplicaciones personales y las fotografías de tus familiares".

Los empleados deben formar parte de este compromiso: Deben saber apreciar el valor de cooperar con el departamento de TI para poder usar las herramientas a las que están acostumbrados, y ayudar a sentar las bases de un proceso que permitirá adoptar con más rapidez las nuevas tecnologías en el lugar de trabajo a medida que surjan.

Otro ajuste fundamental que deben realizar las empresas y sus equipos de seguridad radica en la aceptación de la naturaleza pública de los negocios. Según el estudio *Connected World [Mundo Conectado],* los jóvenes profesionales y los estudiantes distinguen menos límites entre la vida laboral y la personal: El 33% de los estudiantes universitarios sostienen que no tienen problemas en compartir información personal por Internet.

"La generación anterior supone que todo es privado, salvo lo que deciden dar a conocer al público", explicó David Evans, futurista en jefe de Cisco. "Para la generación más joven, todo es público, salvo lo que deciden mantener en privado. Esta posición por defecto —"todo es público"— contradice la forma en que las empresas solían trabajar en el pasado. Hasta ahora han competido e innovado basándose en la idea de que necesitan proteger su información y evitar su divulgación. Sin embargo, es preciso que comprendan que los beneficios derivados del uso compartido de la información son mayores que los riesgos de mantener la información confinada puertas adentro".

La buena noticia para los departamentos de TI es que su función como facilitadores de la colaboración y el uso compartido debería traducirse en una mayor responsabilidad —y con suerte, en un mayor presupuesto— a la hora de lograr el crecimiento y desarrollo de la empresa. "Se logra el éxito cuando el departamento de TI puede habilitar estos cambios radicales en el lugar de trabajo y no impedirlos", señaló John N. Stewart, vicepresidente y director de seguridad de Cisco. "No tenemos que centrarnos en problemas específicos, por ejemplo, si debemos permitir o no que los empleados usen sus iPads en el trabajo, porque el resultado es evidente. Lo que tenemos que hacer es centrarnos en encontrar soluciones para el mayor desafío empresarial: Aprovechar la tecnología para obtener una ventaja competitiva".

Sus futuros empleados:
Equipados con dispositivos y no muy preocupados por la seguridad

Hace diez años se les entregaban laptops a los empleados y se les indicaba que no debían perderlas. Luego se les entregaban las credenciales para tener acceso a la red de la compañía y se les indicaba que no debían decirle a nadie su contraseña. En eso consistía toda la capacitación en seguridad.

Hoy en día, sin embargo, sus empleados de la "generación del milenio", las personas que usted desea contratar por las nuevas ideas y energía que pueden aportar a su empresa, se presentan en su primer día de trabajo con sus propios teléfonos, tablets y laptops, y esperan integrar esos dispositivos en su vida laboral. También esperan que otros (es decir, el equipo de TI y los directores de información) eluciden la manera en que pueden usar sus preciosos dispositivos en cualquier momento y lugar que deseen sin poner en riesgo a la empresa.Piensan que la seguridad no es en realidad su responsabilidad: lo que ellos quieren es trabajar mucho, desde su casa u oficina, usando las redes sociales y aplicaciones en la nube para realizar sus tareas, y que otra persona se encargue de incorporar seguridad transparente en sus interacciones.

La investigación del estudio *Connected World* ofrece un resumen de cómo los jóvenes profesionales y estudiantes universitarios que están por ingresar en la fuerza laboral conciben la seguridad, el acceso a la información y los dispositivos móviles. A continuación ofrecemos una instantánea de sus futuros empleados, basada en los hallazgos del estudio:

EL **81%** DE LOS ESTUDIANTES UNIVERSITARIOS CONSIDERAN QUE DEBEN PODER ELEGIR LOS DISPOSITIVOS **QUE NECESITAN** PARA TRABAJAR

Fuente: *Cisco Connected World Technology Report*

Medios sociales: hoy, una herramienta de productividad

Hace tiempo que Facebook y Twitter dejaron de ser sitios novedosos para adolescentes y geeks, y se convirtieron en canales imprescindibles para comunicarse con grupos y promocionar marcas. Los jóvenes profesionales y estudiantes universitarios lo saben e incorporan los medios sociales en todos los aspectos de su vida. (Si bien Facebook y Twitter son los actores dominantes en gran parte del mundo, muchas otras redes sociales regionales están adquiriendo vital importancia para las interacciones por Internet, por ejemplo Qzone en China, VKontakte en Rusia y los países del ex bloque soviético, Orkut en Brasil y Mixi en Japón.)

Sin embargo, es posible que las empresas no comprendan el nivel con el que han penetrado los medios sociales en la vida pública y privada de sus empleados, en particular, los más jóvenes. Por este motivo, no sienten la necesidad de satisfacer la creciente demanda de su fuerza laboral de contar con un acceso sin límites a las redes sociales como Facebook o a sitios de uso compartido de contenido como YouTube. Lamentablemente, esta inercia puede costarles los talentos que necesitan para crecer y lograr el éxito. De no brindarse el acceso a redes sociales, es probable que los jóvenes profesionales que esperan contar con ese acceso busquen trabajo en otras empresas que sí lo hagan. Estas actitudes son aun más comunes entre los estudiantes universitarios, que desde niños utilizan los medios sociales.

Según la investigación del estudio *Connected World*, los estudiantes universitarios y los jóvenes empleados centran sus interacciones sociales y profesionales en Facebook. El 89% de los estudiantes universitarios encuestados visitan su página de Facebook, al menos, una vez por día, y también lo hace el 73% de los jóvenes profesionales. En el caso de los jóvenes empleados, sus conexiones en los medios sociales suelen extenderse al ámbito laboral: Siete de cada 10 empleados señalaron que se hicieron amigos de gerentes o compañeros de trabajo en el sitio del medio social.

Dado su nivel de actividad en Facebook –y la falta de distinción entre el uso personal y profesional de los sitios de medios sociales–, se infiere que los jóvenes empleados también desean usar Facebook en la oficina. Entre los estudiantes universitarios encuestados, casi la mitad (un 47%) señaló que considera que las empresas deben mantener políticas flexibles relativas a los medios sociales, probablemente para que los empleados puedan mantenerse conectados en su vida laboral y personal en cualquier momento.

Si los estudiantes se topan con un lugar de trabajo que desalienta el uso de medios sociales, es posible que eviten esas empresas, y si están trabajando en esos entornos, es posible que traten de subvertir las reglas que bloquean el acceso a sus sitios favoritos. Más de la mitad de los estudiantes universitarios encuestados a nivel mundial (56%) señalaron que si encontraban una empresa que prohibía el acceso a los medios sociales, no aceptarían el empleo o lo aceptarían pero tratarían de encontrar la manera de acceder a los medios sociales pese a las políticas de la empresa. Además, dos de cada tres estudiantes universitarios (64%) dijeron que pensaban consultar sobre las políticas de uso de medios sociales en sus entrevistas laborales, y uno de cada cuatro (24%) señaló que las políticas de ese tipo serían un factor fundamental a la hora de tomar una decisión y aceptar un puesto de trabajo.

La ventaja del acceso a los medios sociales

Dado que los medios sociales ya están tan incorporados en la vida diaria de los jóvenes profesionales y los futuros empleados, las empresas no pueden seguir considerándolos como una molestia pasajera o una fuerza negativa y disruptiva. De hecho, es probable que las empresas que impiden o restringen el acceso a los medios sociales pierdan competitividad.

Cuando las empresas aceptan que sus empleados utilicen los medios sociales, ponen a su alcance las herramientas, y la cultura, que necesitan para aumentar su productividad, su capacidad de innovación y su competitividad. Por ejemplo, los gerentes de recursos humanos pueden usar las redes sociales para reclutar nuevos talentos. Los equipos de marketing pueden supervisar los canales de medios sociales para seguir el éxito de las campañas publicitarias o la opinión de los consumidores respecto de las marcas. Por su parte, los equipos de atención al cliente pueden responder a los consumidores que utilizan los medios sociales para hacer preguntas y brindar sus opiniones y comentarios a las empresas.

Los temores respecto de la seguridad y la pérdida de datos son la principal razón por la cual las empresas no adoptan los medios sociales; sin embargo, es probable que esos temores sean desproporcionados frente al verdadero nivel de riesgo (consulte “Mito frente a Realidad: Los medios sociales son peligrosos para la empresa” en la página siguiente). En todo caso, los riesgos pueden mitigarse

[1] “The Evolution of Koobface: Adapting to the Changing Security Landscape,” Cisco 2010 Annual Security Report, www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf.

mediante la aplicación de controles tecnológicos y del usuario. Por ejemplo, los controles del tráfico web pueden detener software malicioso como Koobface1 que se filtra por Facebook y Twitter. Estos controles no impiden a los empleados navegar por los medios sociales y utilizarlos para conectarse con colegas, clientes y partners empresariales. Se interrumpe su actividad en los medios sociales solo si corren el riesgo de descargar un archivo infectado o hacer clic en un enlace sospechoso. La protección es invisible para los usuarios y está integrada en la red, no en las computadoras ni en los dispositivos. Los empleados obtienen el acceso a los medios sociales que quieren y las empresas obtienen la seguridad de la información que necesitan. (En "El futuro de las políticas de uso aceptable" en la página 19, encontrará más información sobre las protecciones para medios sociales.)

Los propios sitios de medios sociales han respondido a los pedidos de mayores niveles de control respecto de lo que los usuarios pueden ver en una red. Por ejemplo, una empresa puede permitir a sus empleados acceder a YouTube para ver videos relacionados con su sector o producto y bloquear el acceso a sitios con contenidos para adultos o de juegos de azar. Además, las soluciones tecnológicas pueden filtrar el tráfico de medios sociales para detectar programas maliciosos entrantes o datos salientes (por ejemplo, los archivos de la empresa que no deben enviarse a través de medios sociales u otros servicios de Internet).

Para proteger a los usuarios de una empresa contra el acceso no autorizado a sus cuentas, Facebook implementa constantemente distintas funciones de privacidad. Si bien se trata de controles del usuario y no controles de la red, las empresas pueden intercambiar ideas con sus empleados y ofrecerles capacitación sobre las funciones más útiles para mantener la seguridad de la información.

Antes de limitar el acceso a los medios sociales, es conveniente que las empresas evalúen su valor empresarial frente al riesgo de autorizar su uso. Considerando los hallazgos del estudio Connected World y la pasión que tienen los jóvenes empleados por los medios sociales y su poder de colaboración, es probable que las empresas descubran que las ventajas superan los riesgos, con tal de que logren encontrar el equilibrio adecuado entre su aceptación y la seguridad.

Mito frente a **Realidad**: Los medios sociales son peligrosos para la empresa

Mito:
Al permitir a los empleados usar los medios sociales, se abren las puertas al software malicioso en la red de la empresa y, en consecuencia, la productividad disminuye de manera pronunciada. Además, los empleados divulgarán en Facebook y Twitter chismes internos y secretos de la empresa, lo que dañará su posición competitiva.

Realidad:
No cabe duda de que los delincuentes han utilizado las redes de medios sociales para inducir a sus víctimas a descargar software malicioso y a revelar sus contraseñas de acceso. Sin embargo, el temor a las amenazas que se distribuyen por los medios sociales puede ser exagerado; los mensajes de correo electrónico siguen siendo la forma más popular de introducir software malicioso en las redes.

Sin duda, las empresas deben preocuparse por la pérdida de propiedad intelectual; no obstante, los medios sociales no merecen que se les atribuya toda la culpa por esas pérdidas. Los empleados que no han recibido capacitación para proteger la información del empleador pueden dar a conocer secretos mediante charlas indiscretas en lugares públicos o por correo electrónico con la misma rapidez con la que envían tweets, y pueden descargar documentos de la empresa en pendrives (memorias USB) con la misma facilidad con la que intercambian información por el correo de Facebook. La respuesta a la fuga de propiedad intelectual no consiste en prohibir todos los medios sociales, sino en infundir confianza a los empleados para que no se sientan obligados a divulgar información de carácter confidencial.

"La pérdida de productividad a causa de las redes sociales ha sido el tema de muchas historias alarmistas en los medios de prensa", señaló Jeff Shipley, gerente de Investigación y Operaciones de Seguridad de Cisco. "Sin embargo, lo cierto es que los empleados pueden trabajar más, mejor y con mayor rapidez cuando usan las herramientas que les permiten colaborar de inmediato en proyectos y hablar con los clientes. Hoy, esas herramientas son las redes de medios sociales. El aumento de la productividad compensa el tiempo de inactividad ocasional inherente a la interacción en esas redes".

> "Lo cierto es que los empleados pueden trabajar más, mejor y con mayor rapidez cuando usan las herramientas que les permiten colaborar de inmediato en proyectos y hablar con los clientes".
>
> —Jeff Shipley, gerente de Investigación y Operaciones de Seguridad de Cisco

Acceso remoto y estrategia BYOD:

Empresas que trabajan para encontrar puntos en común con los empleados

Aunque la pregunta de si permitir a los empleados acceder a los medios sociales en el horario de trabajo y con los recursos de la empresa es prioritaria para muchas organizaciones, una preocupación más apremiante es lograr encontrar el equilibrio adecuado entre permitir a los empleados tener acceso a las herramientas y la información que necesitan para hacer bien sus tareas, en cualquier momento y lugar, y mantener protegida la información confidencial de la empresa, como la propiedad intelectual y la información personal de los empleados.

Las empresas de todos los sectores han comenzado a comprender que deben adaptarse pronto a la "consumerización de TI" (la introducción y adopción por parte de los empleados de dispositivos de consumo en la empresa) y las tendencias de trabajo a distancia que ya se están implementando en sus organizaciones. Resulta cada vez más claro que si no cambian, no podrán mantener su competitividad, innovar, conservar una fuerza laboral productiva ni atraer y mantener a los mejores talentos. A mismo tiempo, las empresas comprenden que ya no es posible mantener más los límites de seguridad definidos con anterioridad. "Las organizaciones de TI, en especial las de las grandes empresas, no logran mantenerse a la par del vertiginoso crecimiento de los nuevos dispositivos y la adopción inmediata de esos dispositivos por parte de los empleados, en particular los más jóvenes", destacó Gavin Reid, Gerente del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) de Cisco.

Es clara la expectativa que existe entre los jóvenes profesionales del futuro, y los de hoy, de que podrán tener acceso a todo lo que necesitan desde cualquier lugar para trabajar. Y si no se les proporciona ese acceso, las consecuencias para la empresa pueden ser notables. A título ilustrativo podemos señalar que en el estudio *Connected World* se reveló que tres de cada 10 jóvenes profesionales en el mundo admite que la ausencia de acceso remoto influiría en sus decisiones laborales, como dejar antes un puesto de trabajo o rechazar de plano ofertas laborales. También indican que sería más probable que disminuyera su productividad laboral y se viera afectado su estado de ánimo.

Respecto de los estudiantes universitarios actuales, la mayoría de ellos ni siquiera puede imaginar una experiencia laboral futura que no incluya la posibilidad de acceder al trabajo a distancia. Según la encuesta *Cisco Connected World Technology*, casi dos de cada tres estudiantes universitarios esperan poder acceder a la red de la empresa con la computadora de su casa cuando trabajen. Además, alrededor del 50% de los estudiantes universitarios esperan hacerlo con sus dispositivos móviles personales. Y si la empresa no les permite hacer esas cosas, es más que probable que estos futuros empleados encuentren la manera de superar los obstáculos al acceso.

En el informe también se indica que la mayoría de los estudiantes universitarios (71%) comparten la idea de que los dispositivos que entregan las empresas deben estar disponibles para el trabajo y la diversión porque "el tiempo de trabajo suele combinarse con el tiempo personal... Así funcionan las cosas hoy y así lo harán en el futuro". Esta última afirmación encierra una gran verdad; por este motivo aumentan las empresas que han comenzado a implementar

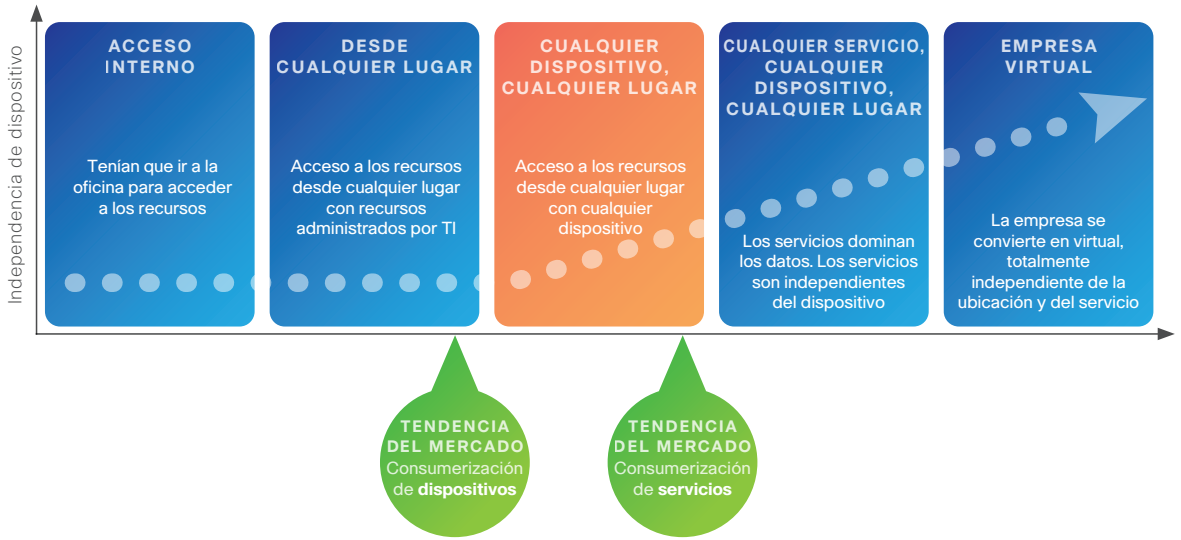


Figura 1. Fases del acceso de los empleados a lo largo de la transición a un entorno que admite cualquier dispositivo

una estrategia BYOD (trae tu propio dispositivo). Otros factores, como la movilidad de la fuerza laboral, la proliferación de nuevos dispositivos y la adquisición, integración y administración de relaciones con proveedores externos, también desempeñan un papel fundamental.

Cisco es una organización que ya está realizando la transición a un entorno BYOD y está aprendiendo con rapidez que esta transformación exige un compromiso multidisciplinario y de largo plazo en la organización. En la figura 1 de la página anterior se ilustran las cinco fases del acceso de los empleados junto con lo que Cisco denomina la transición a un entorno que admite "cualquier dispositivo" para convertirse en una "empresa virtual". Para cuando Cisco llegue a la última fase de su transición planificada, que durará varios años, la organización será más independiente de la ubicación y del servicio, y los datos de la empresa seguirán protegidos.2

Las demandas específicas del segmento al que pertenece una organización (demandas normativas) y la cultura de la empresa (tolerancia del riesgo frente a innovación) son factores que influyen en las decisiones de implementar una estrategia BYOD. "Pienso que para muchas organizaciones hoy la cuestión de la estrategia BYOD no gira tanto en torno a "no, no podemos hacerlo", sino más bien en torno a las preguntas "*¿Cómo lo hacemos?* ¿Qué medidas positivas y flexibles debemos adoptar para administrar la situación de los dispositivos móviles en nuestra organización?", planteó Nasrin Rezai, director senior de arquitectura de seguridad y director del Grupo Empresarial de Colaboración de Cisco.

Entre las organizaciones que avanzan en la implementación de una estrategia BYOD se observa que existe apoyo de los máximos ejecutivos, que no solo ayudan a dar prioridad al tema en la empresa, sino que también

La tecnología permite realizar una transición más segura a BYOD en Cisco

Como parte de la decisión de permitir a los empleados que utilicen cualquier dispositivo para trabajar, incluidos los dispositivos personales no administrados, el departamento de TI de Cisco, junto con CSIRT, buscó una herramienta que bloqueara los sitios web maliciosos antes de que se cargaran en los navegadores. En resumidas cuentas, quería protección contra las amenazas de día cero, en particular contra las que no tienen una firma conocida. Sin embargo, la solución también debía preservar la experiencia del usuario, no solo para garantizar la productividad, sino también para evitar que los empleados cambiaran la configuración del navegador.

El departamento de TI de Cisco y CSIRT lograron ese objetivo al implementar el dispositivo de seguridad en línea (WSA) Cisco IronPort® S670, un proxy web que inspecciona y reenvía o descarta el tráfico web basándose en filtros de reputación o el resultado de la exploración de archivos en línea. (Cisco no utiliza las funciones de filtrado web de WSA para bloquear todas las categorías de sitios web porque su política consiste en confiar en que sus empleados utilizarán su tiempo de manera productiva.)

Cuando un empleado hace clic en un enlace o ingresa en una dirección URL, la solicitud se envía a través de Web Cache Communication Protocol (WCCP) a un grupo de carga equilibrada de dispositivos WSA Cisco IronPort S670. El dispositivo WSA determina si autoriza o rechaza todo el sitio web, o algunas de sus partes, basándose en la puntuación de la reputación de Cisco IronPort SenderBase Security Network (www.senderbase.org), el servicio de supervisión del tráfico web y de correo eléctrico en la nube. SenderBase® asigna a cada sitio web una puntuación de reputación que oscila de –10 a 10. Los sitios web con una puntuación de –6 a –10 se bloquean automáticamente, sin exploración. Los sitios web con una puntuación de 6 a 10 se autorizan, también sin exploración.

Cisco implementó el dispositivo WSA Cisco IronPort S670 en toda su organización en tres fases, que comenzaron con un programa de prueba de concepto de seis meses de duración en un edifico del campus de Cisco en Research Triangle Park (RTP), Carolina del Norte, seguido de un programa piloto de dos años de duración (2009–2011) en el que la solución se amplió a los 3000 empleados del campus de RTP. En 2011, el dispositivo WSA se implementó en otros campus de gran dimensión situados en distintas ciudades del mundo y alcanzó a decenas de miles de empleados. Hasta octubre de 2011, se había finalizado un 85% del proyecto de implementación de WSA en Cisco a nivel mundial.

"Cisco está experimentando el máximo nivel de protección en su historia contra amenazas de la web", destacó Jeff Bollinger, investigador senior de seguridad de la información de Cisco. "Registramos en promedio 40 000 transacciones bloqueadas por hora. Y en tan solo un día, los dispositivos WSA bloquearon 7,3 millones de transacciones, así como 23 200 intentos de descarga de troyanos, más de 6 800 troyanos, 700 gusanos y casi 100 direcciones URL de phishing".

Obtenga más información sobre la implementación de WSA Cisco IronPort S670 en Cisco en www.cisco.com/web/about/ ciscoitatwork/downloads/ciscoitatwork/pdf/cisco_it_ case_study_wsa_executive_summary.pdf.

[2] Para acceder a otros consejos sobre la adopción del modelo BYOD y obtener más información sobre las cinco fases de la transición de Cisco a un entorno que admite "cualquier dispositivo", consulte Cisco Any Device: Planning aProductive, Secure and Competitive Future [Cualquier dispositivo en Cisco: Plantificación de un futuro productivo, seguro y competitivo], www.cisco.com/en/US/solutions/collateral/ns170/ns896/white_paper_c11-681837.pdf.

impulsan su concreción. Rezai explicó: "Los ejecutivos están desempeñando un papel vital a la hora de impulsar la adopción de una estrategia BYOD en la empresa. Están aceptando el riesgo del caos, pero también están diciendo: "Vamos a hacer esto de manera sistemática y arquitectónica, y vamos a evaluar los avances a lo largo de todo el proceso". (Consulte "Preguntas a hacerse a lo largo de la propia transición a un entorno que admite "cualquier dispositivo" en la página siguiente.)

La gobernanza también es crucial para el éxito de una estrategia BYOD. Por ejemplo, Cisco cuenta con un comité ejecutivo de BYOD, dirigido por el departamento de TI e integrado por las principales partes interesadas de otras unidades de negocio, como recursos humanos y legales. Sin una estructura formal de gobernanza, las empresas no pueden definir un camino claro para que la organización pase de manera estratégica y satisfactoria de un mundo administrado a uno no administrado o "sin fronteras", donde se esfuma el perímetro de seguridad y el departamento de TI no administra todos los recursos tecnológicos en uso en la organización.

"Muchas personas piensan que una estrategia BYOD tiene que ver con puntos terminales solamente; sin embargo, es mucho más que eso", señaló Russel Rice, director de administración de productos de Cisco. "Se trata de garantizar la uniformidad de la experiencia del usuario que trabaja con cualquier dispositivo, ya sea en un entorno de red fija o inalámbrica, o en la nube. Se trata de los elementos de interacción de la política. Y se trata de los datos, cómo se protegen y cómo atraviesan estos entornos diferentes. Se deben tener en cuenta todas estas cosas al adoptar una estrategia BYOD; en realidad, supone un cambio de mentalidad."

Mito frente a **Realidad**: Los empleados no aceptarán el control de sus dispositivos móviles por parte de la empresa

Mito:
Los empleados no aceptarán el requisito de que el empleador ejerza cierto grado de control a distancia del dispositivo móvil personal que desean utilizar para el trabajo y la diversión.

Realidad:
Las empresas y los empleados deben buscar puntos en común; la empresa ha de reconocer la necesidad de cada persona de utilizar el dispositivo que prefiere y el empleado ha de comprender que la empresa debe hacer todo lo necesario para implementar su política de seguridad y cumplir con las obligaciones normativas en materia de seguridad de datos.

Las organizaciones deben poder identificar dispositivos únicos cuando entran en la red empresarial, vincular los dispositivos con los usuarios específicos y controlar la posición de seguridad de los dispositivos utilizados para conectarse a los servicios de la empresa. Está evolucionando la tecnología que permitiría "contener" los dispositivos, es decir, un teléfono virtual en un teléfono que el empleador podría apagar en caso de robo o pérdida del dispositivo, sin poner en peligro la integridad de los datos personales del usuario, que se mantienen separados. Cabe esperar que en los próximos años se dispondrá de soluciones de seguridad viables basadas en esta tecnología para su uso generalizado en la empresa.

Hasta entonces, los empleados que deseen utilizar su dispositivo personal preferido para trabajar deberán aceptar que la empresa, por razones de seguridad, conserva determinados derechos a fin de proteger el dispositivo. A tal fin, exigirá, entre otros elementos los siguientes:

- **Contraseñas**
- **Cifrado de datos** (como cifrado del dispositivo y de medios desmontables)
- **Opciones de administración a distancia** que permiten al departamento de TI bloquear o limpiar a distancia un dispositivo en caso de robo, pérdida u otro tipo de afectación, o en caso de desvinculación del empleado.

Si un empleado no acepta los requisitos de implementación de políticas de seguridad y administración de recursos, creados para elevar un dispositivo móvil a la categoría de "confiable" según los estándares de seguridad de la empresa, en ese caso el departamento de TI no permitirá al empleado acceder con su dispositivo preferido a los recursos protegidos de la empresa.

Preguntas a hacerse a lo largo de la propia transición a un entorno que admite “cualquier dispositivo”

Cuando Cisco comenzó su transición a un entorno que admite “cualquier dispositivo”, identificó 13 áreas de negocio cruciales, afectadas por este nuevo paradigma. En la siguiente tabla se destacan esas áreas prioritarias y se ofrece una lista de preguntas que han ayudado a Cisco a identificar, y evitar, posibles problemas, y determinar el mejor enfoque de estos aspectos. Las empresas que desean adoptar una estrategia BYOD también deben considerar estas preguntas[3]

Área de negocio	Preguntas empresariales a responder
Planificación de la continuidad empresarial y recuperación tras desastres	¿Debe permitirse o restringirse el acceso de dispositivos que no pertenecen a la empresa en la planificación de continuidad empresarial? ¿Se debe poder limpiar a distancia cualquier dispositivo terminal que accede a la red en caso de pérdida o robo?
Administración de hosts (aplicación de revisiones)	¿Se permitirá a los dispositivos que no pertenecen a la empresa que se unan a los flujos de administración de host existentes en la organización?
Configuración de clientes, administración y validación de seguridad de dispositivos	¿Cómo se validará y mantendrá actualizada la conformidad del dispositivo con los protocolos de seguridad?
Estrategias de acceso a distancia	¿Quién tiene derecho a acceder a qué servicios y plataformas, y con qué dispositivos? ¿Se deben otorgar a un empleado temporal los mismos privilegios respecto de dispositivos terminales, aplicaciones y datos?
Licencias de software	¿Debe modificarse la política para permitir la instalación de software con licencia de la empresa en dispositivos que no le pertenecen? ¿Los contratos de software vigentes dan cuenta de los usuarios que tienen acceso a la misma aplicación de software a través de varios dispositivos?
Requisitos de cifrado	¿Los dispositivos que no pertenecen a la empresa deben cumplir con los requisitos vigentes de cifrado de disco?
Autenticación y autorización	¿Se esperará o permitirá que los dispositivos que no pertenecen a la empresa se unan a los modelos existentes de Microsoft Active Directory?
Administración del cumplimiento de la normativa vigente	¿Cuál será la política de la organización respecto del uso de dispositivos que no pertenecen a la organización en situaciones de alto riesgo o con elevados requisitos normativos?
Administración e investigaciones de accidentes	¿Cómo administrará el departamento de TI los incidentes y las investigaciones de seguridad y privacidad con dispositivos que no pertenecen a la empresa?
Interoperabilidad de aplicaciones	¿Cómo manejará la organización las pruebas de interoperabilidad de aplicaciones con dispositivos que le no pertenecen?
Administración de recursos	¿La organización debe modificar su método de identificación de sus propios dispositivos para identificar también los que no le pertenecen?
Asistencia	¿Cuáles serán las políticas de la organización para proporcionar asistencia a dispositivos que no le pertenecen?

[3] Ibid.

Distribución de dispositivos móviles en la empresa y ataques de software malicioso

El estudio *Connected World* reveló que tres de cada cuatro empleados en todo el mundo (77%) tienen varios dispositivos, como una laptop y un smartphone, o varios teléfonos y computadoras. El 33% de los jóvenes profesionales (uno de cada tres) señaló que utilizan tres dispositivos para el trabajo, como mínimo. Ahora bien, ¿qué plataformas de dispositivos móviles prefiere la mayoría de los empleados hoy, en general?

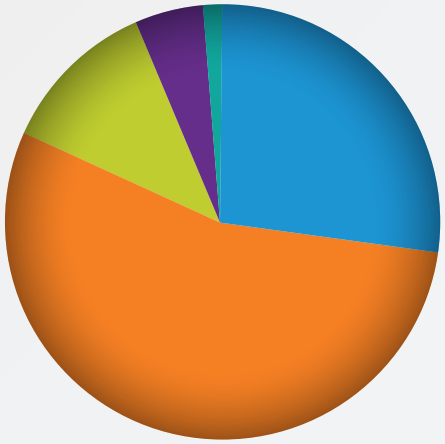
A fin de realizar la investigación para el *Informe Mundial de Cisco sobre Amenazas* más reciente, Cisco ScanSafe analizó de cerca los tipos de plataformas de dispositivos móviles que los empleados de todo el mundo utilizan en la empresa.* Sorprende observar que los dispositivos RIM BlackBerry, que desde hace tiempo se aceptan en la mayoría de los entornos empresariales, representan la cuarta plataforma más popular entre los empleados.

Quizás, sorprende aun más observar que los dispositivos táctiles iPhone, iPad e iPod de Apple Inc. son, en este momento, la plataforma más dominante. Google Android ocupa el segundo puesto, y los dispositivos Nokia/Symbian ocupan el tercero.** Estos resultados subrayan el potente impacto que ha tenido la consumerización de TI en las empresas en un breve período: El primer iPhone se introdujo en el mercado en 2007; el primer teléfono equipado con Android se introdujo en el mercado en 2008.

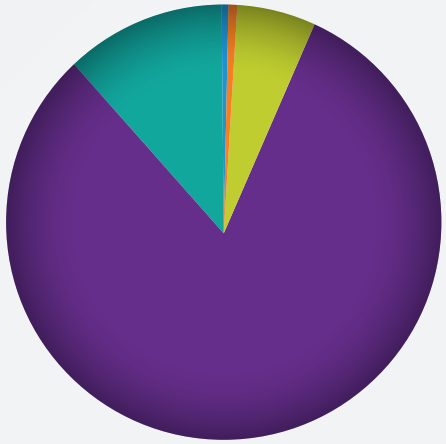
La investigación de Cisco ScanSafe también ofrece información sobre las plataformas de dispositivos móviles que se enfrentan a software malicioso. La respuesta: Todas ellas. (Consulte el siguiente gráfico.) Si bien en este momento los dispositivos BlackBerry experimentan la mayoría de los ataques (más del 80%), la investigadora senior de amenazas a la seguridad, Mary Landesman, de Cisco señaló que el software malicioso no tiene como objetivo específico ni dispositivos ni usuarios de BlackBerry, y es dudoso que el software malicioso encontrado haya infectado o tenido otro impacto en esos dispositivos.

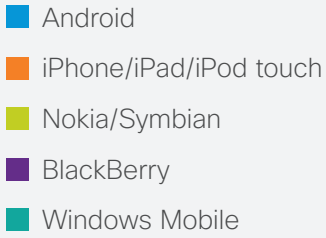
Landesman agregó: "A dondequiera que vayan los usuarios, los ciberdelincuentes los seguirán. A medida que siga aumentando el uso de dispositivos móviles entre los usuarios empresariales, también aumentarán los programas maliciosos dirigidos a esos dispositivos, y a sus usuarios. (Para obtener más información sobre el aumento de la inversión de los ciberdelincuentes en explotaciones que se dirigen a usuarios de dispositivos móviles, consulte la "Matriz de Cisco del Retorno de la inversión de la ciberdelincuencia (CROI)" en la página 26.)

Uso de dispositivos móviles por la empresa



Distribución normalizada de ataques





Source: Cisco ScanSafe

* Cisco ScanSafe procesa miles de millones de solicitudes web por día. Los resultados del estudio se basan en un análisis de los agentes de usuario normalizados por cantidad de clientes.

** Dispositivos Nokia/Symbian lanzados al mercado en octubre de 2011.

La revolución del iPad: Tablets y seguridad

Cuando en 2010 se lanzó al mercado la computadora tablet iPad de Apple, se posicionó (y el público la adoptó) como dispositivo de consumo: Ya que entre los casos de uso favoritos se encontraban ver películas con los hijos, navegar por la web sentado en un sofá y leer libros.

Sin embargo, muchos sectores, como el de salud y el de manufactura, apreciaron de inmediato el atractivo de un potente dispositivo móvil fácil de usar con fines profesionales que salvaría las diferencias entre los smartphones (demasiado pequeños) y las laptops (demasiado grandes). En una reciente conferencia sobre los resultados económicos de la empresa, el director financiero de Apple señaló que el 86% de las empresas Fortune 500 y el 47% de las empresas Global 500 están implementando o probando el iPad; empresas tales como General Electric Co. y SAP están desarrollando aplicaciones específicas para el iPad para sus procesos internos; y los pilotos de Alaska Airlines y American Airlines utilizan el iPad en las cabinas para sustituir la información de navegación en formato impreso.[4]

Al mismo tiempo, los empleados que utilizan el iPad y otras tablets en su casa solicitan a sus empleadores que les permitan usar los dispositivos en la oficina; otro hito de la consumerización de TI. Este fenómeno se ve reflejado en el estudio Cisco Connected World, según el cual el 81% de los estudiantes universitarios esperan poder elegir el dispositivo para su trabajo, y recibir presupuesto para adquirir los que prefieren o llevar sus propios dispositivos personales.

Ya sea que las empresas o los empleados impulsen la adopción de los iPads y otras tablets, lo cierto es que los dispositivos suscitan preguntas e inquietudes respecto de la protección de la información de la empresa a la que se accede a través de tablets. A diferencia de los smartphones, los iPads y las tablets ofrecen plataformas de computación más sólidas, en las cuales los empleados pueden lograr más que con los smartphones. Las empresas con visión de futuro desean poder incorporar las tablets, sin sacrificar la seguridad.

La innovación ha suscitado cambios constantes en TI y el ritmo de cambio está aumentando. Las empresas que diseñan su estrategia de dispositivos basándose en el dispositivo más popular de 2011 (en este caso, el iPad) tendrán que comenzar a programar la reingeniería de sistemas para dentro de unos pocos años, cuando surjan nuevos proveedores, productos, características y funciones. Una decisión más estratégica radica en escindir el tema de la seguridad de dispositivos

específicos y enfocarse en una estrategia de habilitación de BYOD con el acceso basado en usuario, función y tipo de dispositivo (en la página página 10 encontrará más información sobre la estrategia BYOD). La clave para habilitar cualquier dispositivo en la empresa, ya sea que el dispositivo pertenezca a la empresa o el empleado lo traiga de su casa, consiste en la administración de identidad, que supone comprender quién utiliza el dispositivo, dónde lo utiliza y a qué información tiene acceso. Por otra parte, las empresas que adoptan el uso de tablets en el lugar de trabajo necesitarán métodos de administración de dispositivos (p. ej., para borrar datos de dispositivos perdidos), como los que tienen para los smartphones y las laptops.

Respecto de las tablets, y en realidad, de cualquier dispositivo nuevo y genial que se incorpore en la empresa en el futuro, los profesionales de seguridad deben preservar la experiencia del usuario aunque añadan funciones de seguridad. Por ejemplo, a los usuarios de los iPads les encantan los controles de la pantalla táctil, como mover los dedos por la pantalla para ver imágenes o agrandarlas. Si los departamentos de TI incorporan funciones de seguridad que restringen estas apreciadísimas características, los usuarios se resistirán a los cambios.

"El mejor enfoque de la seguridad de tablets es aquel que permite aislar las aplicaciones y los datos empresariales y personales de forma confiable, aplicando la política de seguridad adecuada para cada uno", explicó Horacio Zambrano, gerente de productos de Cisco. "La política se implementa en la nube o con una red inteligente, mientras que se mantiene la experiencia del usuario y el empleado puede aprovechar las funciones propias de las aplicaciones del dispositivo".

[4] "Apple's corporate iPhone, iPad app strength bad news for rivals" ZDNet, 20 de julio de 2011, www.zdnet.com/blog/btl/apples-corporate-iphone-ipad-app-strength-bad-news-for-rivals/52758.

La influencia de los dispositivos móviles, los servicios en la nube y los medios sociales en la política de seguridad de la empresa

El costo de tan solo una violación de datos puede ser elevadísimo para una empresa. Según estimaciones de Ponemon Institute, el costo oscila entre USD1 millón y USD58 millones.5 El costo no solo es de carácter económico: El daño a la reputación de la empresa y la pérdida de clientes y de participación de mercado son posibles efectos secundarios de un incidente de pérdida de datos de alto perfil.

A medida que aumenta la cantidad de empleados móviles que utilizan varios dispositivos para acceder a los recursos de la empresa y aplicaciones de colaboración para trabajar con otras personas mientras se encuentran fuera de los "cuatro muros" tradicionales de la empresa, también aumentan las posibilidades de pérdida de datos. A título ilustrativo podemos mencionar que en el estudio Cisco Connected World (www.cisco.com/en/US/ netsol/ns1120/ index.html) se determinó que casi la mitad de los jóvenes profesionales (46%) envían mensajes profesionales de correo electrónico a través de cuentas personales.

"Las posibilidades de pérdida de datos son elevadas", señaló David Paschich, gerente de productos de seguridad web de Cisco. "Las empresas vienen perdiendo constantemente el control de los usuarios que tienen acceso a la red empresarial. Y el simple hecho de que una cantidad mayor de empleados utiliza dispositivos móviles en el trabajo, y a veces, varios dispositivos, supone que son más elevadas las posibilidades de pérdida de datos a causa del robo o la pérdida de un dispositivo".

La creciente preferencia de los ciberdelincuentes por el uso de ataques dirigidos de bajo volumen, como las campañas de spearphishing (consulte: Actualización sobre correo no deseado a nivel mundial: Disminución radical del volumen de correo no deseado, página 29), para robar información a objetivos de alto valor, y el mayor uso de servicios de distribución de archivos basados en la nube por parte de las empresas para aumentar la eficiencia y reducir los costos (consulte la siguiente sección: Protección de datos de la empresa en la nube) también aumentan las posibilidades de que los datos sean objeto de robo u otro tipo de siniestro.

Ante este panorama, no sorprende el hecho de que más empresas renueven su enfoque en las iniciativas de prevención de pérdida de datos. "Hoy, las empresas evalúan sus programas de prevención de pérdida de datos para determinar dos elementos: Si protegen los datos adecuados y si hacen lo correcto para mantener su seguridad", explicó John N. Stewart, vicepresidente y director de seguridad de Cisco.

Al categorizar los datos cuya seguridad debe mantenerse, un buen punto de partida para muchas organizaciones consiste en determinar los tipos de datos que exigen protección y seguridad en función de la normativa vigente, la que puede variar por sector y región geográfica (p. ej., estado, provincia, país). "No es posible crear anillos de seguridad alrededor de las cosas que deben protegerse si no se sabe cuáles son esas cosas", destacó Jeff Shipley, gerente de Investigaciones y Operaciones de Seguridad de Cisco. "Se trata de un cambio de mentalidad importante en muchas organizaciones que centran los controles de seguridad en los sistemas y la red, y no en la granularidad de los datos reales existentes en los diversos sistemas, entre varios sistemas o la red". Añadió que las empresas no deben omitir la propiedad intelectual al categorizar los datos que deben protegerse.

Shipley también advirtió que los departamentos de TI de las empresas no deben perder oportunidades obvias para evitar que los datos "salgan caminando por la puerta principal". Señaló: "Por ejemplo: si una empresa protege sus archivos de carácter confidencial, como los archivos Excel que contienen datos de los clientes, mediante controles para evitar que se descarguen o muevan los datos de aplicaciones o bases de datos centralizadas, se reducirán en gran medida las posibilidades de que un empleado descargue esos datos en un dispositivo personal o móvil antes de irse de la compañía".

Paschich también advirtió a las empresas que no deben ignorar una amenaza de más bajo perfil pero muy potente a la seguridad de los datos: Los dispositivos USB. "Mientras las empresas se preocupan por si permiten o no que un empleado se conecte a la red con un iPhone porque temen socavar la seguridad, sí permiten que sus empleados conecten dispositivos USB en sus laptops y copien todos los datos que deseen".

Ofreció un consejo más para fortalecer la protección de los datos en la empresa: Establecer medidas de prevención de pérdida de datos y políticas de uso aceptable en documentos separados. "Estas iniciativas se interrelacionan, sin duda, pero son diferentes", explicó Paschich. (Consulte "El futuro de las políticas de uso aceptable" en la página 19.)

Protección de datos de la empresa en la nube

La distribución de archivos en la nube es un método popular y práctico para compartir archivos de gran tamaño por Internet, y representa otra área de riesgo posible para la seguridad de los datos de la empresa. La idea de que se transfiera información empresarial confidencial entre servicios en la nube basados en la web, que no administra la empresa, puede quitar el sueño a los profesionales de seguridad.

[5] *Email Attacks: This Time It's Personal*, Cisco, June 2011, www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.

La distribución de archivos en la nube está ganando terreno debido a su facilidad de uso: El proceso de acceso a servicios como Box.net o Dropbox es rápido y sencillo; para utilizar los servicios no es necesario contar con hardware o software avanzado y los servicios son gratuitos o de bajo costo.

Además, simplifican la colaboración entre empleados y asesores externos o partners, dado que los archivos pueden compartirse sin generar métodos engorrosos y complejos para tener acceso a las redes empresariales. Los jóvenes empleados, que están programados para depender de los servicios en la nube, como el correo web y las redes sociales, no dudarán en adoptar el uso compartido de archivos en la nube e impulsarán su adopción generalizada en la empresa.

La cesión del control de los datos empresariales a la nube, en particular a una parte de la nube que escapa al control de la empresa, suscita interrogantes legítimos sobre la seguridad de la información. "Muchos proveedores nuevos en este mercado son empresas "startup" con escasa experiencia en la prestación de servicios para toda la empresa y con los desafíos que esto pone al descubierto", señaló Pat Calhoun, vicepresidente y gerente general de la Unidad de Negocio de Servicios de Redes Seguras de Cisco. "Además, los estándares de seguridad y cifrado pueden variar ampliamente de un proveedor a otro. Las ventajas del uso compartido de archivos en la nube son numerosas; pero las empresas deben hacer preguntas difíciles a los proveedores de este servicio respecto de sus políticas para mantener la seguridad".

Entre esas preguntas podemos señalar las siguientes:

- ¿Qué tipo de controles de cifrado ofrece el proveedor?
- ¿Qué personal tiene acceso a los datos del cliente?
- ¿Quién administra la supervisión y respuesta a incidentes: el proveedor o el cliente?
- ¿El proveedor subcontrata algunos servicios? ¿Los proveedores subcontratados almacenan en caché los datos?
- ¿Se han implementado políticas de prevención de pérdida de datos?
- ¿El proveedor realiza evaluaciones periódicas de la seguridad?
- ¿Qué medidas de redundancia existen? ¿Cómo y dónde se almacenan los archivos de copia de seguridad?

Además de evaluar a los proveedores, las empresas que prevén establecer una política relativa al uso compartido de archivos en la nube deberán adoptar las siguientes medidas:

Crear un sistema para clasificar los datos. Los documentos pueden clasificarse por nivel de confidencialidad; por ejemplo, "público", "confidencial", "sumamente confidencial", etc., según las necesidades de la organización. Se deberá capacitar a los empleados en cómo aplicar esas designaciones, y comprender cómo pueden afectar a la posibilidad de compartir archivos en la nube.

Crear un sistema para manejar datos especializados. Los datos que poseen implicancias legales o de cumplimiento exigen un manejo especial en términos de políticas de conservación, ubicación física y requisitos de medios de copia de seguridad. Las empresas deben definir políticas respecto del envío de esos datos a personas externas, además de su clasificación por niveles de confidencialidad.

Implementar una solución de prevención de pérdida de datos. Es posible que los proveedores de servicios de distribución de archivos no ofrezcan el nivel detallado de control de prevención que necesitan las empresas. Una solución de prevención de pérdida de datos en la red puede evitar que se carguen los datos en los servicios de distribución de archivos según las clasificaciones, por ejemplo, archivos impositivos o código fuente.

Ofrecer la administración de identidad para controlar el acceso. La red deberá autenticar a los usuarios para que puedan cargar o descargar archivos. Es imprescindible aprovechar la identidad y federación de identidad empresarial para la colaboración interna y externa, y administrar el ciclo de vida de las cuentas provistas.

Definir lo que se espera del proveedor. En el contrato de nivel de servicio (SLA) deben estipularse políticas y servicios claros y definidos; por ejemplo, sistemas y controles de cifrado redundantes, prácticas relativas al acceso a datos por parte de terceros (p. ej., autoridades policiales), que establezcan las responsabilidades compartidas que podrían comprender funciones administrativas, de respuesta y supervisión de incidentes, y actividades de transferencia y depuración de datos antes de la finalización del contrato.

Distribución de dispositivos móviles en la empresa y ataques de software malicioso

En 2011 se registraron varios incidentes de seguridad de datos de alto perfil, que tuvieron como protagonistas a Sony Corp.6 y Citigroup Inc.[7], entre otros, y que motivaron a los legisladores de EE. UU. a sancionar leyes que afectarán a la forma en que las empresas protegen la información de los consumidores y comunican al público los incidentes de ciberseguridad.

En septiembre de 2011 la Comisión de Asuntos Judiciales del Senado estadounidense adoptó y aprobó tres proyectos de ley relativos a la violación de datos y la privacidad; por su parte la Comisión de Comercio del Senado y la de Comercio y Energía de Diputados también están trabajando en distintas versiones de estos proyectos. En el Senado, cualquier versión que se sancione será una solución de compromiso de todas las versiones que aprueben sus comisiones, y tal vez, se incorpore en un proyecto de ley más completo sobre ciberseguridad que circula por el Senado. Las versiones aprobadas por la Comisión de Asuntos Judiciales del Senado son:

Ley de notificación de violaciones de datos de 2011[8]
Esta norma obligaría a los organismos federales y empresas que "realizan actividades de comercio interestatal" y poseen datos que contienen información confidencial de identificación personal a divulgar toda infracción de seguridad.

Ley de protección de datos personales y responsabilidad por infracción[9]
La ley crearía un proceso para ayudar a las empresas a establecer los estándares mínimos adecuados de seguridad para proteger la información de los consumidores de carácter confidencial. También exigiría a las empresas que notifiquen de inmediato a las personas tras una violación de datos.

Ley de privacidad y seguridad de datos personales de 2011[10]
Esta norma crearía un estándar nacional que las empresas deberán seguir al comunicar violaciones de datos. Además, establecería la obligación de las empresas de implementar programas de privacidad y seguridad de la información con el objeto de evitar las violaciones de datos. El proyecto de ley también contempla sanciones de carácter penal.

Para cuando se finalizó el presente informe, los proyectos de leyes federales de notificación de violaciones de datos seguían en trámite en el Congreso de los EE. UU., junto con la legislación integral en materia de ciberseguridad concebida para ayudar a proteger las redes financieras, los sistemas de transporte y las redes de distribución de energía eléctrica. Hace más de un año que el Senado viene trabajando en la legislación integral en materia de ciberseguridad; en mayo de 2011, la administración de Obama compartió su posición sobre lo que debería incluir esa legislación.[11]

[6] "Sony Playstation Suffers Massive Data Breach," de Liana B. Baker y Jim Finkle, Reuters.com, 26 de abril de 2011, www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

[7] "Citi Says Many More Customers Had Data Stolen by Hackers," de Eric Dash, The New York Times, 16 de junio de 2011, www.nytimes.com/2011/06/16/technology/16citi.html

[8] Ley de notificación de violaciones de datos de 2011: www.govtrack.us/congress/billtext.xpd?bill=s112-1408

[9] Ley de protección de datos personales y responsabilidad por infracción: http://judiciary.senate.gov/legislation/upload/ALB11771-Blumenthal-Sub.pdf

[10] Ley de privacidad y seguridad de datos personales: www.govtrack.us/congress/billtext.xpd?bill=s112-1151

[11] "Cartas a las Cámaras de Diputados y Senadores sobre la propuesta de ciberseguridad de la Administración", WhiteHouse.gov, 12 de mayo de 2011, www.whitehouse.gov/sites/default/files/omb/legislative/letters/Cybersecurityletters-to-congress-house-signed.pdf.

El futuro de las políticas de uso aceptable

Muchas políticas de uso aceptable surgieron a partir de la necesidad de las empresas de establecer reglas relativas al acceso a Internet con recursos empresariales por parte de los empleados durante horas laborales. Con el transcurso del tiempo muchas de estas políticas se transformaron en colosales documentos "abarca todo" que regulaban desde el acceso a medios sociales por Internet hasta lo que los empleados no podían decir acerca de su empresa cuando navegaban en línea fuera del horario laboral. En consecuencia, a pesar de las buenas intenciones de estas políticas, a los empleados les costaba internalizarlas y respetarlas, y para las empresas era casi imposible hacerlas cumplir.

De acuerdo con los resultados de la encuesta Cisco Connected World, la mayoría de las políticas de uso aceptable no son eficaces por otro motivo: los empleados no creen que deban ayudar a la empresa a hacer cumplir esas políticas. La investigación indica que tres de cada cinco empleados (61%) no se consideran responsables por la protección de la información y los dispositivos de la empresa; por el contrario, creen que su cuidado está en manos del departamento de TI y/o los proveedores de servicios. Entonces la pregunta es: ¿Cuál es el objetivo de tener una política de uso aceptable?

"Las políticas de uso aceptable son importantes por muchas razones, entre ellas el cumplimiento normativo, pero en su mayoría no son realistas", sostuvo Gavin Reid, gerente de CSIRT de Cisco. "Muchas de ellas no son más que listas interminables, llenas de prohibiciones. Son simplemente un instrumento de la empresa de decirles a sus empleados, al departamento de asuntos legales o a los investigadores ante un incidente de seguridad: "Nosotros le advertimos que no lo hiciera".

Reid aseguró que un mejor enfoque para las empresas sería reformular las políticas de uso aceptable de manera tal de que sean pertinentes y se puedan hacer cumplir, y agregó que muchas organizaciones ya lo están haciendo. Las nuevas políticas de uso aceptable que surgen de este proceso son más simples y sólidas. En general, se trata de listas mucho más cortas (algunas de ellas incluyen solo un puñado de disposiciones, tales como aclarar que los empleados no pueden usar las aplicaciones de par a par (P2P) o enviar correo electrónico no deseado desde sus computadoras de escritorio. Reid destacó que todas las disposiciones de estas listas "pueden hacerse cumplir desde el punto de vista técnico", es decir que la organización cuenta con la tecnología necesaria para identificar violaciones a las políticas en cuestión.

Nilesh Bhandari, gerente de productos de Cisco, sostuvo que "la tendencia actual con las políticas de uso aceptable es que las empresas están adoptando un enfoque mucho más basado en los riesgos". "Las empresas se están concentrando en aquello que sí o sí deben incluir en una política de uso aceptable y lo que es más útil para ellas, en particular en términos del tiempo y los costos necesarios para controlar el cumplimiento de estas políticas por parte de los empleados".

Asimismo, agregó que para los empleados es más fácil comprender y aplicar una política de uso aceptable bien definida, lo cual, a su vez, permite a la empresa aumentar la productividad de su fuerza laboral. "Los usuarios prestarán atención a una política de uso aceptable cuando comprendan cabalmente lo que sucederá si no la cumplen", aseguró Bhandari.

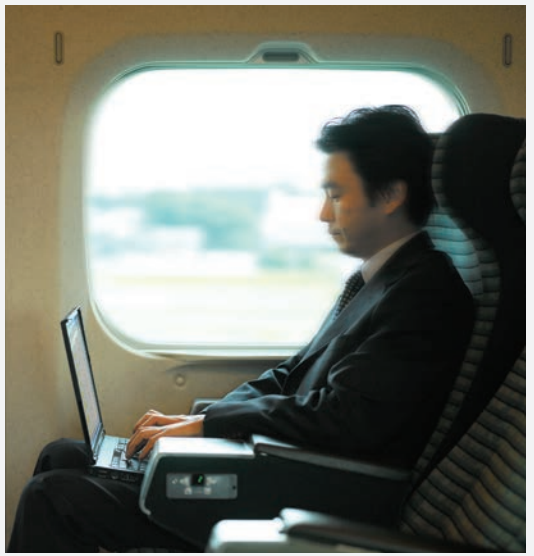
> "La tendencia actual con las políticas de uso aceptable es que las empresas están adoptando un enfoque mucho más basado en los riesgos".
>
> —Nilesh Bhandari, Gerente de Produto, Cisco

Mito frente a **Realidad**: Las políticas de uso aceptable no se pueden hacer cumplir

Myth:
Las políticas de uso aceptable no influyen para nada porque no pueden hacerse cumplir y, para empezar, a las empresas les resulta muy difícil elaborarlas.

Reality:
Las empresas no pueden hacer cumplir políticas muy amplias eficazmente. Si bien se requiere tiempo e investigación para determinar lo que debería incluir una política de uso aceptable y si realmente es posible hacer cumplir cada una de sus disposiciones o no, el resultado final será una política que los empleados podrán entender y cumplir con más facilidad, y que permitirá fortalecer la seguridad de la empresa.

Es importante capacitar a los empleados acerca del uso seguro del correo electrónico y la web dado que se trata de vías que suelen utilizar los ciberdelincuentes para infiltrarse en las redes e infectarlas, robar propiedad intelectual y otros datos de carácter confidencial, y comprometer a los usuarios particulares.



Primeros pasos en seguridad de la colaboración

Las empresas pueden seguir los pasos que se indican a continuación para establecer políticas de seguridad, tecnologías y procesos en materia de colaboración y seguridad de medios sociales:

- **Crear un plan empresarial para soluciones de colaboración** y redes sociales a partir de las necesidades de la empresa.
- **Diseñar mecanismos claros de control de seguridad** para la colaboración.
- **Crear políticas sobre la confidencialidad de la información** y aclarar las expectativas de comportamiento de los empleados cuando interactúan en sitios de colaboración.
- **Definir políticas sobre medidas de seguridad en la red,** tales como acceso remoto mediante dispositivos móviles, nivel de protección de la contraseña y uso del intercambio directo de archivos.
- **Identificar requisitos normativos y de cumplimiento** que podrían restringir el uso de la información o su divulgación en los medios sociales.
- **Crear recursos de capacitación para todos los usuarios.**

Medios sociales: Políticas más controles tecnológicos

A juzgar por los resultados del estudio Connected World, es probable que los estudiantes universitarios y jóvenes profesionales encuentren la manera de evadir las restricciones de acceso a los medios sociales según sus necesidades, independientemente de las políticas de la empresa. Tres de cada cuatro empleados encuestados consideran que sus empresas deberían permitirles acceder a los medios sociales y a los sitios personales con los dispositivos que les entregan para trabajar.

Además, el 40% de los estudiantes universitarios aseguró que violaría las reglas sobre medios sociales de la empresa. Se trata de una porción importante de los posibles futuros empleados encuestados en el marco de este estudio y constituye una advertencia para las empresas que están luchando con sus políticas de uso aceptable para los medios sociales. En otras palabras, se puede prohibir o restringir el uso de los medios sociales, pero existe la posibilidad de que los empleados accedan a ellos de todas maneras.

A las organizaciones con políticas de uso aceptable que limitan el acceso de sus empleados a los medios sociales probablemente les resulte difícil atraer a los jóvenes más idóneos y talentosos. El 29% de los estudiantes encuestados aseguró que no aceptaría una oferta laboral de una empresa que no les permitiera acceder a los medios sociales en horario laboral. Y de aquellos que aceptarían una oferta de este tipo, solo el 30% aseguró que cumpliría con la política indicada.

"El acceso a los medios sociales y la libertad de elección de la tecnología pasarán a ser un beneficio decisivo para los empleados más jóvenes que estén considerando dónde comenzar sus carreras", afirmó Chris Young, vicepresidente senior del Grupo de Seguridad de Cisco.

"Las organizaciones de recursos humanos deben incluir estos factores en la cultura y la política corporativas para mantener una ventaja competitiva. Las empresas deberían establecer un punto medio factible entre el deseo de los empleados de compartir y las necesidades de la empresa de mantener la seguridad informática, los datos, la privacidad y la protección de los recursos".

Dicho punto medio incluye permitir el acceso a los medios sociales y otras tecnologías de colaboración y, a su vez, utilizar controles tecnológicos para desviar amenazas, tales como mensajes de software malicioso o "phishing". En general, son los usuarios los que controlan las configuraciones de seguridad de las redes sociales y no los departamentos de TI. A los efectos de compensar esta falta de control, se pueden implementar medidas de seguridad adicionales, por ejemplo, un sistema de prevención de intrusiones para proteger contra amenazas a la red y un sistema de filtrado basado en la reputación para detectar actividades y contenidos sospechosos.

Junto con los controles tecnológicos, debería ofrecerse capacitación a los usuarios que aclare las expectativas de la empresa respecto de las prácticas y comportamiento apropiados para acceder a medios sociales desde los dispositivos o las redes de la empresa. Según se mencionó anteriormente ("Medios sociales: Hoy, una herramienta de productividad", página 8), los jóvenes profesionales se han acostumbrado tanto a compartir información en los medios sociales que pueden no darse cuenta, o no haber aprendido nunca, que hasta los pequeños datos que se publican en una red social pueden dañar a una empresa. La falta de capacitación de los usuarios acerca de los problemas de seguridad de la colaboración como de pautas para divulgar información en línea puede generar una exposición a este riesgo.

PARTE

2

Panorama de amenazas cibernéticas para 2012: El factor del ciberactivismo pirata

Hoy en día, las empresas se enfrentan con una variedad de problemas de seguridad resultante de las actitudes y los hábitos laborales cambiantes de sus empleados, así como también de la dinámica de un mundo más colaborativo, conectado y móvil. Según lo veremos en esta mitad del Informe Anual de Seguridad de Cisco 2011, las empresas también deben seguir protegiéndose de una amplia gama de serias amenazas de las cuales los ciberdelincuentes ya se están beneficiando e invirtiendo recursos adicionales para perfeccionarlas, tales como las amenazas persistentes avanzadas (APT por sus siglas en inglés), los troyanos para el robo de datos y las vulnerabilidades de la web.

No obstante, las empresas ahora deben considerar otra posible amenaza a la seguridad que podría ser incluso más perjudicial para sus transacciones si fueran blanco de ataque: el "ciberactivismo pirata".

"El ciberactivismo pirata es una transformación de la piratería informática tradicional", explicó John N. Stewart, vicepresidente y director de seguridad de Cisco. "Los piratas informáticos solían actuar por diversión y para alimentar su mala fama. Luego lo hicieron a cambio de un premio o una ganancia monetaria. Hoy, sus actividades suelen tener como objetivo mandar un mensaje, y puede que uno nunca se entere de por qué fue elegido como blanco. Ahora estamos defendiendo un nuevo dominio".

El "ciberactivismo pirata", un término acuñado a partir de "hacking" (piratería informática) y activismo, pasó a ocupar un lugar prioritario entre los problemas de seguridad a fines de 2010 cuando los seguidores de WikiLeaks.org lanzaron ataques de denegación de servicio distribuido (DDoS) contra entidades tales como PayPal y Mastercard. Esta iniciativa recibió el nombre de "Operation Payback" (Operación venganza).[12] De distintas maneras, el "ciberactivismo pirata" es una extensión natural de la manera en la cual las personas utilizan Internet hoy en día: Para conectarse con personas con ideas afines en todo el mundo. Internet es una plataforma poderosa para quienes desean expresarse y captar la atención de una audiencia amplia, así como también para motivar a otros para que actúen de manera similar. (Consulte "Los medios sociales ejercen el poder de "reunión"". Esta sección se encuentra en la página opuesta.)

Detrás de "Operation Payback" había un grupo conocido como el colectivo Anonymous (Anónimo) que desde entonces ha crecido tanto en adhesiones como en influencia en todo el mundo. (Para obtener más información acerca de Anonymous, consulte "Cisco Cybercrime Showcase", en la página 24.) Recientemente, Anonymous se ha conectado con el movimiento Operación Wall Street.[13] Las protestas de los "indignados" comenzaron en la Ciudad de Nueva York pero se expandieron rápidamente para inspirar marchas similares en más de 900 ciudades de todo el mundo. Los activistas que representan a Anonymous incitaron a sus miembros a participar en el movimiento, el cual suele ser pacífico, aunque ha habido choques de violencia con la intervención de las fuerzas de seguridad en algunas ciudades como Roma, Italia,[14] y Oakland, California.[15] En ocasiones, las facciones de Anonymous que se identifican con el movimiento "Ocupa" amenazaron una mayor destrucción con campañas de hacking para detener las operaciones de importantes mercados financieros.

Durante el año pasado, los incidentes de ciberactivismo pirata por parte de otros grupos han contribuido a elevar esta amenaza para que pase a ser una de las principales preocupaciones de las empresas en materia de amenazas informáticas. LulzSec, por ejemplo, hizo hincapié en las fuerzas de seguridad lanzando ataques de denegación de servicio distribuido (DDoS) y robo de datos contra una organización británica cibercriminal y las fuerzas de seguridad de Arizona.[16] En julio, un grupo relacionado llamado "Script Kiddies" realizó un ataque informático a las cuentas de Twitter de Fox News y anunció el asesinato del Presidente Barack Obama.[17]

El "ciberactivismo pirata" puede ocurrir rápidamente y sin aviso, aunque Anonymous sí anunció algunos de sus objetivos, tales como HBGary Federal, una empresa contratada por el gobierno federal de los EE. UU. para detectar a los ciberactivistas que atacan a organizaciones que habían retirado el respaldo de WikiLeaks.org. Si bien la amenaza del ciberactivismo pirata puede parecer remota, es muy real y representa un cambio en la naturaleza de la ciberdelincuencia propiamente dicha.

"Un principio rector para la creación de la estrategia de seguridad ha sido comprender los móviles del delito. No obstante, la finalidad de caos total de los ciberactivistas piratas socava este modelo dado que cualquiera puede atacar a cualquier empresa por cualquier motivo" explicó Patrick Peterson, investigador en seguridad de Cisco. "Lo que una empresa intentaría proteger ante una violación "tradicional" a la seguridad, como la propiedad intelectual, puede no ser del interés de este tipo de hacker. El "valor" de esta acción consiste en que el hacker en cuestión logre dañar, avergonzar o hacer un ejemplo de su objetivo, o todo lo anterior".

Stewart agregó "prever un incidente de ciberactivismo pirata significa crear un plan de acción claro que detalle lo que una organización diría y haría después de sufrir un incidente de este tipo. El desarrollo de este plan debería ser una labor multidisciplinaria que incluya a la gerencia, los equipos de seguridad, el departamento de legales y hasta los profesionales en comunicaciones. Si su empresa sufre este tipo de situaciones, debe manejarlas adecuadamente dado que el daño que sufra su marca puede ser duradero. Tal como sucede con tantas cosas, debe estar preparado y contar con un plan antes de sufrir un incidente".

[12] "'Anonymous' Launches DDoS Attacks Against WikiLeaks Foes," de Leslie Horn, PCMag.com, 8 de diciembre de 2010, www.pcmag.com/article2/0,2817,2374023,00.asp#fbid=jU1HvGyTz7f.

[13] Página Web de Occupy Wall Street: http://occupywallst.org/.

[14] "Occupy protests spread around the world; 70 injured in Rome," de Faith Karimi y Joe Sterling, CNN.com, 15 de octubre de 2011, www.cnn.com/2011/10/15/world/occupy-goes-global/index.html.

[15] "Occupy Oakland Violence: Peaceful Occupy Protests Degenerate Into Chaos", Associated Press, The Huffington Post, 3 de noviembre de 2011, www.huffingtonpost.com/2011/11/03/occupy-oakland-violence-_n_1073325html.

[16] "Lulzec Release Arizona Law Enforcement Data, Claims Retaliation for Immigration Law", de Alexia Tsotsis, TechCrunch.com, 23 de junio de 2011, http://techcrunch.com/2011/06/23/lulzsec-releases-arizona-law-enforcementdatain-retaliation-for-immigration-law/.

[17] "Script Kiddies Hack Fox News Account, Tweet Obama's Death", de Nicholas Jackson, The Atlantic, 4 de julio de 2011, www.theatlantic.com/technology/archive/2011/07/script-kiddies-hack-fox-news-account-tweet-obamas-death/241393/.

Tendencias geopolíticas: Los medios sociales ejercen el poder de "reunión"

Si alguien todavía necesitaba pruebas de que los medios sociales pueden desencadenar cambios en la sociedad a una velocidad impresionante, el 2011 fue el año en que este poder quedó demostrado definitivamente. Las protestas de la "Primavera árabe" a comienzos del año, al igual que las revueltas posteriores en Londres y otras ciudades británicas, demostraron la manera en que los medios sociales pueden movilizar a la gente como ningún medio anterior hubiera sido capaz. En ambos casos, se utilizó Twitter y Facebook para garantizar la asistencia a las reuniones públicas, lo que provocó, también en ambos casos, que diversas entidades gubernamentales propusieran bloquear el acceso a los medios sociales restringiendo el acceso a Internet o interviniendo los registros de las cuentas personales de los usuarios.

En un estudio de septiembre de 2011, realizado por la Universidad de Washington, se observó que los medios sociales, en especial Twitter, "desempeñaron un papel central a la hora de orientar los debates políticos durante la Primavera árabe", sobre todo en Egipto y Túnez, según el resumen del estudio. "Las conversaciones acerca de la revolución muchas veces fueron seguidas de sucesos clave en el campo de acción, y los medios sociales difundieron historias inspiradoras de las protestas más allá de las fronteras internacionales".18 Quienes observan los medios sociales esperan que esta tendencia continúe, a medida que la frustración antigubernamental descubre la manera de manifestarse a través de las redes sociales.[19]

Para las empresas y su seguridad, las consecuencias radican en la posibilidad de que se usen los medios sociales para provocar conflictos dentro de las propias organizaciones o contra sus marcas o industrias. (Consulte "Panorama de amenazas cibernéticas para 2012: El factor del ciberactivismo pirata" en la página 22.) "La sensación de anonimato en línea aumenta el riesgo de que haya consecuencias involuntarias si los denominados "ciudadanos de la red" creen tener la libertad de acusar sin necesidad de corroborar sus razones", explicó el analista de amenazas mundiales de Cisco, Jean Gordon Kocienda.

"Para las empresas y los ejecutivos, especialmente en el entorno mundial actual de frustración con quienes son vistos como grupos privilegiados, esto aumenta las probabilidades de que haya problemas de seguridad tanto físicos como virtuales". Por otro lado, cabe esperar que las empresas atraviesen interrupciones comerciales serias si tienen oficinas o empleados radicados en zonas objeto de este tipo de conflictos, dado que el gobierno puede, por ejemplo, interrumpir el acceso a Internet como medida de seguridad. También es posible que se apunte contra aquellas organizaciones que sean vistas como cómplices de un régimen corrupto, o que sufran consecuencias negativas si se piensa que están tratando de reprimir un movimiento revolucionario.

Otro posible problema que las empresas observan es la tendencia cada vez mayor entre las organizaciones gubernamentales a intentar bloquear los medios sociales o incluso los servicios de Internet a gran escala, o exigir el acceso a información de cuentas de usuario o dispositivos móviles que normalmente es privada. Por ejemplo, durante las revueltas en el Reino Unido, las personas usaban BlackBerry Messenger (BBM), el servicio de mensajería instantánea para usuarios de BlackBerry, para intercambiar información acerca de los sitios que iban a saquear o los lugares en donde se reunirían para protestar. BBM es un servicio cifrado de mensajería de teléfono a teléfono que, en general, a las autoridades les resulta más difícil rastrear. RIM, el creador del BlackBerry, accedió a cooperar con los grupos de policía del Reino Unido para tratar de identificar a los usuarios de BBM que apoyaran las revueltas o saqueos, aunque la empresa no aclaró qué tipo de información de las cuentas de BBM iba a difundir.[20]

Una vez pasadas las revueltas, varios funcionarios británicos advirtieron que en el futuro el gobierno podría solicitar una ampliación de los poderes de la policía con el fin de frenar los disturbios, y propusieron pedirles a los proveedores de medios sociales que limiten el acceso a sus servicios durante este tipo de situaciones de emergencia.

Twitter respondió aludiendo a una entrada de su blog de principios de 2011, en el cual se afirmaba el compromiso de la empresa por mantener el servicio sin importar qué tipo de situaciones revolucionarias se estuvieran discutiendo a través de los tweets: "No siempre estamos de acuerdo con las cosas que la gente discute en Twitter, pero garantizamos el flujo de información independientemente de nuestra opinión acerca del contenido".[21]

Los especialistas en seguridad prevén una disputa de poder entre los gobiernos, que exigirán un acceso cada vez mayor a los datos de los usuarios para mantener la ley y el orden, y los defensores de la privacidad, que repudiarán cualquier tipo de concesión de esta naturaleza por parte de los proveedores de tecnología. Por ejemplo, India ha manifestado su preocupación ante la incapacidad del Estado de acceder a este tipo de información (para rastrear, entre otros delitos, la actividad terrorista), y ha llegado a un acuerdo con RIM según el cual el gobierno puede solicitar los datos privados de determinados usuarios en función de cada caso. Varios países de la Unión Europea ya han implementado la Directiva sobre la protección de datos, que fue creada en 2006 y exige que se conserven los datos de las comunicaciones en caso de que los necesiten las autoridades encargadas de hacer cumplir la ley. Sin embargo, otros países de la UE aún no lo han hecho.[22]

"Lo que sí es evidente es que los gobiernos de todo el mundo están tratando, con mucha dificultad, de aplicar los nuevos hechos de la tecnología y las comunicaciones a los principios subyacentes del Derecho y de la sociedad", observó Adam Golodner, director de política de seguridad y tecnología mundial de Cisco. "Esto es lo que siempre ha sucedido cada vez que la tecnología avanza, y en lo que respecta a la cibernética, este intento de armonizar las nuevas realidades y los viejos principios será el principal desafío que enfrentarán las políticas en el futuro cercano".

[18] "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?," Project on Information Technology and Political Islam, http://pitpi.org/index.php/2011/09/11/opening-closed-regimes-what-was-the-role-of-socialmedia-during-the-arab-spring/.

[19] "U.K. social media controls point to wider 'info war'", Reuters, 18 de agosto de 2011, www.reuters.com/article/2011/08/18/us-britain-socialmedia-idUSTRE77H61Y20110818.

[20] "London Rioters' Unrequited Love For BlackBerry", FastCompany.com, 8 de agosto de 2011, www.fastcompany.com/1772171/london-protestors-unrequited-love-for-blackberry.

[21] "The Tweets Must Flow", blog de Twitter, 28 de enero de 2011, http://blog.twitter.com/2011/01/tweets-must-flow.html.

[22] "Sweden postpones EU data retention directive", The Register, 18 de marzo de 2011, www.theregister.co.uk/2011/03/18/sweden_postpones_eu_data_retention_directive/.

Anuncio de los ganadores de 2011 de Cisco Cybercrime Showcase

Siempre habrá héroes y villanos, y el sector de la seguridad no es la excepción. El reparto de los personajes puede cambiar, pero año tras año los actores maliciosos hacen sus máximos esfuerzos por encontrar maneras nuevas de robar dinero e información y hacer desastres a través de los canales en línea, y quienes combaten el delito cibernético están trabajando incansablemente para frustrar sus planes. En esta tercera edición de nuestro Cisco Cybercrime Showcase anual, una vez más quisiéramos identificar a los representantes de ambos bandos, el "bueno" y el "malo", de la batalla por la seguridad, quienes han tenido un impacto notable en el mundo de la ciberseguridad, para bien o para mal, durante el año pasado.

EL BUENO
MICROSOFT

La tecnología de Microsoft siempre ha llamado la atención de los delincuentes debido a su amplia difusión en el mundo de las empresas y entre los consumidores. En particular, los propietarios de botnets han abusado del sistema operativo Windows recurriendo a la ingeniería social, los ataques basados en la web y puntos vulnerables sin revisiones o parches. En los últimos años, Microsoft ha luchado contra los botnets principalmente de tres maneras.

En primer lugar, Microsoft ha mejorado de forma drástica la seguridad de sus productos. Entre los principales desarrollos cabe mencionar la búsqueda intensiva de puntos vulnerables y los ciclos de revisiones semanales; la implementación del Microsoft Security Development Lifecycle (SDL) para aumentar de forma radical la seguridad de los productos; los sistemas de actualizaciones automáticas para todos los productos de software de Microsoft; los cambios importantes en Windows Internet Explorer, como la implementación de un nuevo modelo de seguridad para los controles ActiveX; y el desarrollo de la herramienta de eliminación de software malicioso (Malicious Software Removal Tool/MSRT), que elimina con precisión el malware de la PC. Esta herramienta se ha utilizado contra las familias de software malicioso que están detrás de más de 150 de los botnets más grandes del mundo, como Zeus (Zbot), Cutwail, Waledac y Koobface, para eliminar cientos de millones de infecciones de software malicioso de sistemas informáticos. Las investigaciones de Cisco han demostrado que año tras año los kits de herramientas de vulnerabilidades web son cada vez menos eficaces a la hora de abusar de las tecnologías de Microsoft.

En segundo lugar, Microsoft ha liderado la comunidad de seguridad en la lucha contra el ciberdelito. La unidad de delitos digitales de Microsoft organiza el consorcio anual sobre delitos digitales (DCC), que ofrece la oportunidad para que funcionarios de las fuerzas del orden y miembros de la comunidad de seguridad tecnológica intercambien ideas sobre las iniciativas tendientes a combatir el ciberdelito a nivel mundial. El evento de este año contó con 340 participantes provenientes de 33 países.

En tercer lugar, Microsoft ha promovido acciones legales enérgicas contra los ciberdelincuentes. En 2010, Microsoft promovió una acción judicial para detener el botnet Waledac, que había infectado cientos de miles de computadoras en todo el mundo y enviaba mil quinientos millones de mensajes de correo no deseado por día, y solicitó a un juzgado federal que emitiera una orden de restricción contra casi 300 dominios de Internet que se consideraban controlados por delincuentes relacionados con Waledac. Esta medida interrumpió las comunicaciones entre los centros de mando y control del botnet y sus computadoras afectadas, "aniquilando" con eficacia el botnet.[23]

A principios de 2011, los abogados de Microsoft y comisarios de EE. UU. procedieron a incautar los servidores de mando y control del botnet Rustock, que se encontraban en las sedes de varios proveedores de alojamiento web distribuidos en todo el territorio de los Estados Unidos. El software malicioso diseminado por Rustock, que era utilizado por delincuentes rusos y, en general, distribuía correo no deseado sobre productos farmacéuticos falsos, disminuyó de forma radical hasta que la actividad del botnet cesó por completo. Por otra parte, Microsoft ofreció una recompensa de doscientos cincuenta mil dólares por información que contribuyera a la detención de los creadores de Rustock.24 Según Cisco IronPort SenderBase Security Network, desde que se eliminó el botnet Rustock, el volumen diario de correo no deseado disminuyó de forma radical en todo el mundo.

En septiembre de 2011, Microsoft recurrió a tácticas legales similares para detener el botnet Kelihos, y en la presentación judicial por primera vez hubo un demandado real y se denunció al presunto propietario del dominio web que controlaba e botnet.[25]

Las acciones de Microsoft contra los botnets, combinadas con las cantidades sin precedentes de revisiones para puntos vulnerables, que también contribuyen a acabar con la actividad delictiva, la han convertido en un activista de primer orden contra el ciberdelito. El proyecto MARS (Microsoft Active Response for Security) de la empresa, que supervisa las iniciativas orientadas a desactivar los botnets, también ha compartido sus hallazgos sobre los botnets con miembros del sector de seguridad.

[23] "Deactivating botnets to create a safer, more trusted Internet," Microsoft.com: www.microsoft.com/mscorp/twc/endtoendtrust/vision/botnet.aspx.

[24] "Rustock take-down proves botnets can be crippled, says Microsoft," Computerworld.com, 5 de julio de 2011, www.computerworld. com/s/article/9218180/Rustock_take_down_proves_botnets_can_be_crippled_says_Microsoft.

[25] "How Microsoft Took Down Massive Kelihos Botnet," The Huffington Post, 3 de octubre de 2011, www.huffingtonpost.com/2011/10/03/microsoft-kelihos-botnet_n_992030.html.

EL MALO

ANONYMOUS

Anonymous, que se describe como una "comunidad en línea descentralizada que actúa de forma anónima y coordinada" es una "coalición informal de habitantes de Internet" que funciona desde hace varios años; pero que últimamente está acaparando los titulares de las noticias porque el grupo está cada vez más vinculado con el ciberactivismo pirata de colaboración internacional. (Para obtener más información, consulte "Panorama de amenazas cibernéticas para 2012: El factor del ciberactivismo pirata" en la página 22.)

Quienes se identifican con el colectivo Anonymous están ubicados en distintas ciudades del mundo y se comunican entre sí a través de foros de Internet, imageboards y otros sitios web como 4chan, 711chan, Encyclopedia Dramatica, canales IRC e incluso sitios comunes como YouTube y Facebook. "Es un grupo bastante bien organizado, aunque de afiliación informal", señaló Patrick Peterson, investigador senior de seguridad de Cisco. "Los participantes son sumamente talentosos y ambiciosos. En muchos casos, sus acciones no tienen una motivación lucrativa. Se trata más bien de 'Mira lo que puedo hacer'. Y cuando terminan, se separan y desparecen con la misma rapidez con la que se unieron".

En 2011, Anonymous estuvo vinculado con varios incidentes de hacking de alto perfil, algunos anunciados con antelación y todos destinados a manifestarse; los incidentes fueron ataques directos a los sitios web de:

- Numerosas organizaciones de las fuerzas del orden de EE. UU., que se tradujeron en la divulgación de información personal confidencial de informantes y miembros de dichas fuerzas.
- El gobierno de Túnez, como parte del movimiento "Primavera árabe" (consulte "Tendencias geopolíticas: Los medios sociales ejercen el poder de "reunión"" en la página 23)
- HBGary Federal, organización de seguridad
- Sony Computer Entertainment America

¿Qué amenaza plantea Anonymous de cara al futuro? "Este grupo posee la capacidad para provocar daños reales", señaló Scott Olechowski, gerente de investigaciones sobre amenazas de Cisco. "Hasta ahora la mayoría de las acciones que he visto de ellos no han sido demasiado extremas, han acarreado más molestias que el daño real del que son capaces. En este momento se los podrían definir como traviesos. Pero si se suman algunas personas al colectivo Anonymous que realmente desean provocar daño o si el grupo lleva las cosas demasiado lejos al tratar de manifestarse, podría haber un problema real".

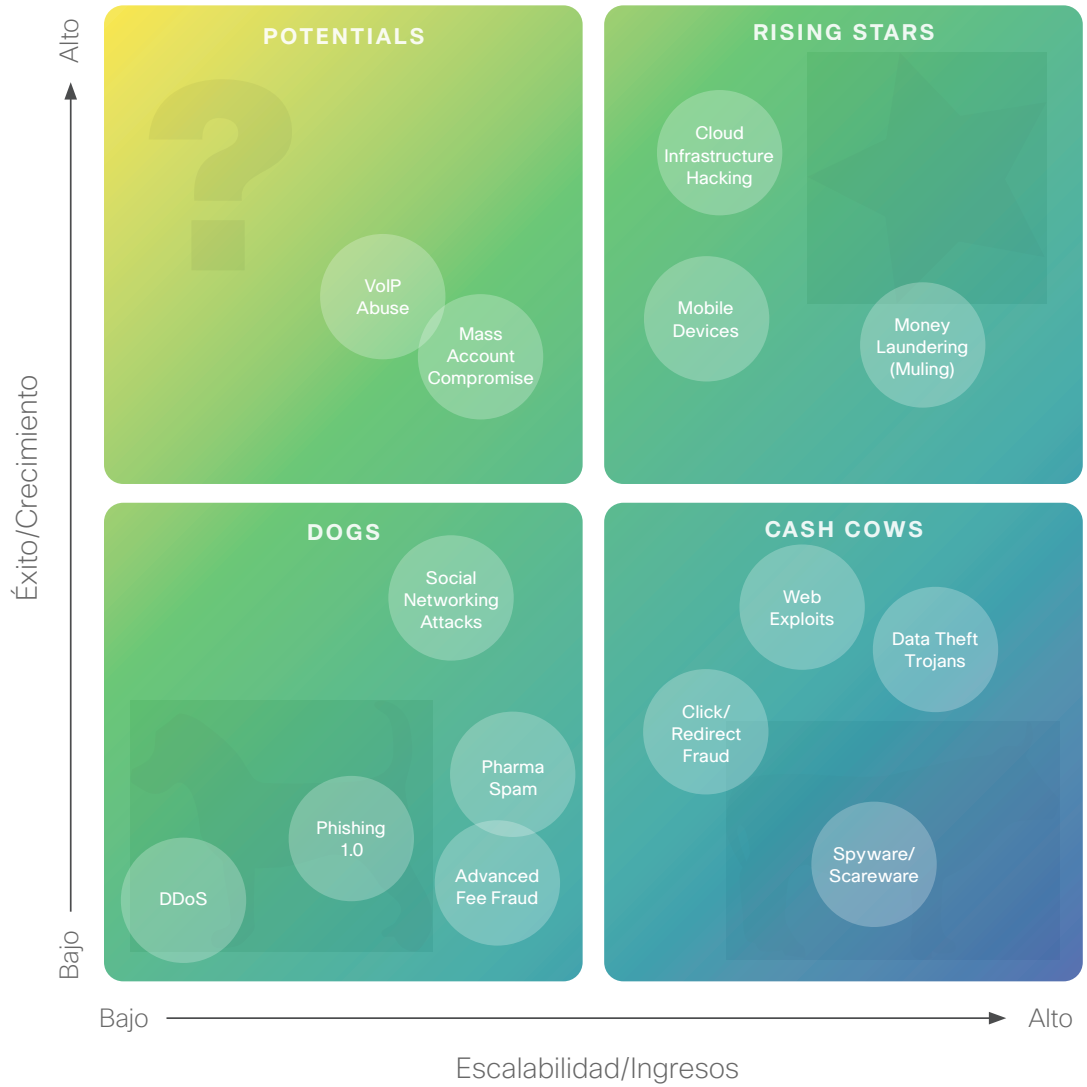
Considere este casi incidente que podría haber sido un gran golpe en una economía mundial ya incierta: En octubre, facciones de Anonymous apuntaron alto al amenazar con "borrar" la bolsa de valores de Nueva York el 10 de octubre de 2011, mediante un ataque de DDoS distribuido en una muestra de apoyo al movimiento Ocupa Wall Street.27 Una posible razón por la cual el grupo no cumplió su promesa de dejar inoperativa la bolsa es que "el llamado a acción atrajo la crítica de adherentes y detractores por igual, y la mayoría condenaba la iniciativa".28 Por ende, parecería que Anonymous, conectado débilmente como está ahora, puede ser influido por su conciencia colectiva de no provocar daños graves, al menos en este caso.

> "Los participantes son sumamente talentosos y ambiciosos. En muchos casos, sus acciones no tienen una motivación lucrativa. Se trata más bien de 'Mira lo que puedo hacer'".
>
> —Patrick Peterson, investigador senior de seguridad de Cisco

[27] "'Anonymous' Hackers Group Threat to New York Stock Exchange," de Ned Potter, ABC News, 10 de octubre de 2011, http://abcnews.go.com/Technology/anonymous-hackers-threaten-erase-york-stock-exchangesite/story?id=14705072.

[28] "Blink and You Missed It: Anonymous Attacks NYSE", de Chris Barth, Forbes.com, 10 de octubre de 2011, www.forbes.com/sites/chrisbarth/2011/10/10/blink-and-you-missed-it-anonymous-attacks-nyse/.

Matriz de Cisco del Retorno de la inversión de la ciberdelincuencia (CROI)



La matriz de CROI de Cisco predice las técnicas de ciberdelincuencia que serán "ganadoras" y "perdedoras" en 2012.

La matriz de CROI de Cisco observa el rendimiento de las operaciones cibercriminales con motivaciones lucrativas, que se administran y organizan cada vez más de formas similares a sofisticadas empresas legítimas. Esta matriz destaca específicamente los tipos de acciones agresivas en las que, según proyecciones de los especialistas de seguridad de Cisco, es probable que los ciberdelincuentes centren la mayoría de sus recursos para desarrollarlas, perfeccionarlas e implementarlas en el próximo año.

Posibles: El compromiso masivo de cuentas, una nueva categoría de la Matriz de CROI de Cisco de este año, básicamente consiste en que los ciberdelincuentes "utilizan las migajas que quedan del robo de datos", según Patrick Peterson, investigador senior de seguridad de Cisco. Unen información recopilada con los troyanos utilizados para el robo de datos a fin de extraer credenciales de bajo valor como nombres de usuario y contraseñas. Se utilizan las credenciales como "trampolín" para volver a utilizarlas en un sitio valioso de servicios bancarios por Internet, o para utilizar las credenciales del correo web y espiar el correo personal de la víctima a fin de sentar las bases de una acción más agresiva. "Los ciberdelincuentes analizan las toneladas de información que recopilan de otra manera. Ahora piensan: ¿El nombre de usuario y la contraseña de este correo web o de este sitio de citas que tengo podría ser la llave para entrar en una cuenta de alto valor? O ¿podría ser un trampolín para explotar un correo web que me va a permitir hacer otras cosas, como restablecer contraseñas y realizar acciones de reconocimiento, que podrían acercarme a premios aun más grandes?" explicó Peterson.

Por otra parte, los ciberdelincuentes están acelerando la inversión en VoIP y otras técnicas de abuso de telefonía. Según el *Informe Anual de Seguridad de Cisco 2010*, muchos delincuentes ya han logrado sus objetivos a la hora de dirigirse a pequeñas o medianas empresas con esta técnica y han provocado considerables pérdidas económicas en algunas organizaciones. El abuso de VoIP, que se indicó como "posible" en la matriz del año pasado, consiste en el hacking de sistemas de central telefónica privada (PBX). Los abusadores de VoIP realizan llamadas de larga distancia fraudulentas, generalmente llamadas internacionales. Algunos delincuentes utilizan sistemas VoIP para realizar estafas más sofisticadas de "vishing" (phishing telefónico), cuyo objetivo es recopilar información confidencial de los usuarios, como números del seguro social. También están aumentando los ataques de spoofing de identificación de llamada contra sistemas de verificación telefónica.

Estrellas Nacientes: Se anticipa que el "lavado de dinero (mulas)" seguirá siendo un área de interés importante para la inversión cibercriminal en 2012. De acuerdo con un análisis detallado del Informe Anual de Seguridad de Cisco 2010, los delincuentes que aprovechan software malicioso para el robo de datos tienen acceso a numerosas cuentas bancarias en línea pero se enfrentan a problemas a la hora de extraer fondos en el exterior sin dejar un rastro directo.29 Las mulas de dinero ofrecen esta solución. Las operaciones con mulas son cada vez más sofisticadas y de alcance internacional. Algunos de los mejores datos proceden de la "Operación Trident Breach", que ha permitido la detención de más de 60 ciberdelincuentes que lograron robar 70 millones de dólares mediante mulas de dinero.30 Si bien se estima que solo una de cada tres transacciones con mulas de dinero son exitosas, y las mulas son fáciles de detener al menos en los Estados Unidos, las redes de mulas siguen creciendo dado que los delincuentes reales disponen de numerosas cuentas bancarias y mulas para explotar.

Un nuevo actor que no sorprende entre las "Estrellas Nacientes" son los dispositivos móviles, que figuraban en la categoría de posibles en la matriz de 2010. Los ciberdelincuentes, en general, centran su atención en el lugar en el que se encuentran los usuarios y las personas acceden cada vez más a Internet, el correo electrónico y las redes empresariales a través de potentes dispositivos móviles. Hace años que los dispositivos móviles son objeto de ataques; no obstante, en una perspectiva histórica, esos ataques nunca fueron generalizados y parecían más proyectos de investigación que operaciones cibercriminales exitosas. Pero ese panorama está cambiando con rapidez.

Las campañas móviles no solo son más comunes, sino también exitosas y, por ende, importante para los ciberdelincuentes. Las nuevas plataformas de SO móviles presentan nuevas vulnerabilidades de seguridad que se pueden explotar. Muchos ciberdelincuentes se benefician mediante aplicaciones móviles falsas que instalan software malicioso. Además, dado que los dispositivos móviles están reemplazando con rapidez las PC tradicionales como herramientas de trabajo, los ciberdelincuentes están invirtiendo más recursos para desarrollar amenazas avanzadas persistentes, explotar la autorización de factor doble y tener acceso a redes empresariales donde pueden robar datos o realizar "misiones de reconocimiento".

Por su parte, mientras aumenta la cantidad de empresas que adoptan el cloud computing y los servicios alojados, los ciberdelincuentes también apuntan a la nube en la búsqueda de oportunidades para lucrar. "Los delincuentes reconocen las posibilidades de obtener un mayor retorno de la inversión con los ataques a la nuble", señaló Scott Olechowski, gerente de investigaciones de amenazas de Cisco. "¿Por qué concentrar todos los esfuerzos en hackear una sola empresa cuando es posible afectar la integridad de la infraestructura alojada y poder acceder a información que pertenece a centenares o incluso miles de empresas?"

Olechowski agregó que los incidentes de seguridad de datos recientes, como el caso de los hackers que acceden a nombres y direcciones de correo electrónico de clientes que están almacenados en los sistemas de la empresa de marketing por correo electrónico Epsilon Data Management LLC31, ponen en evidencia la tendencia creciente a "hackear a uno para hackear a todos".

Vacas lecheras: Dos de las "estrellas nacientes" de 2010 –Troyanos para el robo de datos y vulnerabilidades web– han pasado a integrar la categoría "Vacas lecheras" en 2011, puesto que se encuentran entre las técnicas más lucrativas para los ciberdelincuentes. Sin embargo, este cambio no solo se debe al hecho de que los delincuentes perfeccionaron sus habilidades con estas técnicas; la prevalencia de kits de herramientas de vulnerabilidades web económicos y fáciles de usar, y las explotaciones de troyanos para robar datos supone que cualquier persona que desee entrar en el juego puede hacerlo con relativamente poco esfuerzo o poca inversión. Otros favoritos antiguos como Scareware/Spyware y el fraude de vínculos o redireccionamiento han perdido un poco de brillo; sin embargo, han mantenido su función como leales caballitos de batalla de los ciberdelincuentes durante 2011 y seguirán cumpliendo esa función en 2012.

Perros: Dos nuevos actores de la categoría "Perros" son el correo no deseado farmacéutico y el fraude de pago por adelantado. El correo no deseado farmacéutico, una "vaca lechera" en la matriz de CROI de Cisco de 2010, ha perdido popularidad a causa de las actividades de las fuerzas del orden y el cierre de botnets. (Consulte Cisco Cybercrime Showcase, "El bueno: Microsoft", en la página 24.) Numerosos delincuentes dedicados al correo no deseado farmacéutico se detuvieron o se escondieron para evitar su captura, entre ellos Igor Gusev de SpamIt/Glavmed, Pavel Vrublevsky de RX-Promotions/Eva Pharmacy, Oleg Nikolaenko, operador del botnet masivo Mega-D; Georg Avanesov, operador del botnet Bredolab y muchos otros. Dado que muchos de estos botnets masivos, como Waledac, Mariposa, Cutwail (el mayor botnet de la historia), Rustock, Bredolab y Mega-D, desaparecieron hace tiempo o sufrieron graves daños, y las autoridades vigilan con más atención la posible aparición de spammers, el envío de mensajes de correo no deseado farmacéuticos no les reporta a los ciberdelincuentes las ganancias que solía reportar en el pasado.[32]

Mientras tanto, otra "vaca lechera" del año pasado, el fraude de pago por adelantado, está en vías de extinción. Hoy en día, los usuarios están más informados y los filtros de correo no deseado están mejor ajustados, por lo cual esta técnica ya no ofrece cuantiosas ganancias a las operaciones cibercriminales. La engorrosa estafa "Nigerian Prince" (príncipe nigeriano) sigue circulando, aunque las ganancias siguen disminuyendo.

Los antiguos perros que siguen en la matriz son las estafas Phishing 1.0 y los ataques de DDoS. Los ataques a las redes sociales siguen teniendo un papel secundario ya que los usuarios saben navegar mejor por la "sociosfera" en línea. Muchos más usuarios instintivamente confían menos en otros usuarios que no conocen y que tratan de interactuar con ellos en las redes sociales. También aprovechan los controles de privacidad de los proveedores de redes sociales y, en general, se muestran menos abiertos al compartir información personal en estos sitios. Los ataques a las redes sociales no desaparecerán por completo; no obstante, es improbable que los ciberdelincuentes sofisticados sigan invirtiendo sus recursos para perfeccionar o ampliar ese tipo de vulnerabilidades. Para que funcionen estos tipos de estafas, es preciso trabajar mucho y durante mucho tiempo, en particular hoy que muchos actores de la economía clandestina están haciendo esfuerzos específicos para invertir sus recursos de manera más estratégica.

[29] "'Ibid.

[30] Ukraine Detains 5 individuals Tied to $70 million in U.S. eBanking Heists," Brian Krebs, Krebs on Security blog, 2 de octubre de 2010, http://krebsonsecurity.com/tag/operation-trident-breach/.

[31] "Breach Brings Scrutiny: Incident Sparks Concern Over Outsourcing of Email Marketing," de Ben Worth, The Wall Street Journal, 5 de abril de 2011, http://online.wsj.com/article/SB10001424052748704587004576245131531712342.html.

[32] Para obtener más información sobre el cierre de esos botnets, consulte el Informe Anual de Seguridad de Cisco 2010, www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf.

Análisis de vulnerabilidades y amenazas y actualización sobre correo no deseado a nivel mundial de 2011

El *Informe Anual de Seguridad de Cisco* ofrece una comparación del aumento y la disminución de las vulnerabilidades y amenazas por categoría, así como su impacto estimado.

En el siguiente cuadro de **Categorías de vulnerabilidades y amenazas** se muestra un ligero aumento de las vulnerabilidades y amenazas registradas, una tendencia importante, dado que, en general, venían disminuyendo desde 2008. Un factor que provoca ese aumento son las vulnerabilidades del código o los paquetes de código abierto de los principales proveedores de software, como los que utilizan el motor de navegador de código abierto WebKit. Una sola vulnerabilidad en un producto de código abierto como WebKit puede afectar a varios productos importantes y generar la emisión de advertencias, actualizaciones y revisiones o parches. Este año Apple siguió publicando amplias actualizaciones para varios de sus productos que guardaron relación con la inclusión de software de código abierto.

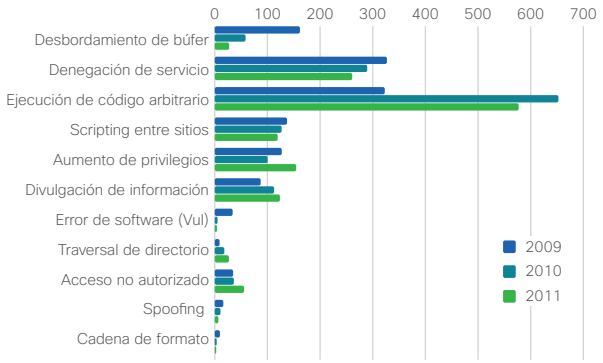
De cara al año 2012, los especialistas en seguridad observan vulnerabilidades en los sistemas de control industrial y los sistemas de adquisición de datos y control de supervisión, denominados también sistemas ICS/SCADA. Estos sistemas representan un área de creciente interés, y las iniciativas gubernamentales de defensa cibernética se enfocan en neutralizar esas vulnerabilidades. Según el *Informe Anual de Seguridad de Cisco 2010*, el gusano de red Stuxnet se creó para infectar y dañar estos sistemas.

La buena noticia de 2011 es la disminución de los errores básicos de codificación: Desbordamientos de búfer, denegación de servicio, ejecución de código arbitrario y vulnerabilidades de cadenas de formato. Sin embargo, esto no incluye las vulnerabilidades y correcciones relacionadas con defectos que permiten ataques de inyección SQL, los que siguen siendo un problema generalizado.

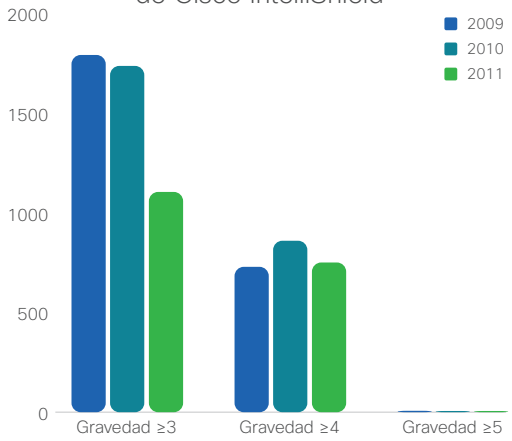
Las clasificaciones del nivel de gravedad de alertas de Cisco IntelliShield reflejan el nivel de impacto de las explotaciones exitosas de puntos vulnerables. En 2011, los niveles de gravedad mantuvieron la tendencia a una ligera disminución, que se observa desde 2009, y refleja las disminuciones recientes de vulnerabilidades y amenazas. Con miras a 2012, se prevé que los niveles de gravedad seguirán siendo los mismos que los actuales y que no habrá ataques ni aprovechamientos generalizados de vulnerabilidades específicas.

Las clasificaciones de urgencia de alertas de Cisco IntelliShield reflejan el nivel de actividad de las amenazas con relación a vulnerabilidades específicas. El año 2011 se caracteriza por un importante aumento del nivel de urgencia 3, lo que significa que se detectó una cantidad limitada de explotaciones aunque podría haber habido otras. Este aumento indica que si bien existe una mayor cantidad de amenazas activas en

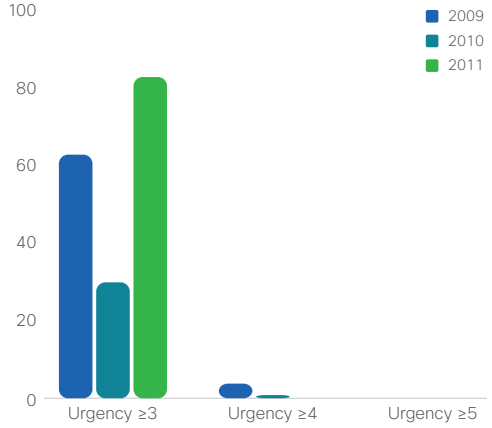
Categorías de vulnerabilidades y amenazas



Clasificaciones de gravedad de alertas de Cisco IntelliShield



Clasificaciones de urgencia de alertas de Cisco IntelliShield



circulación por Internet, en general no trepan al nivel de alertas de urgencia 4 (varios incidentes de explotación se notificaron en diversas fuentes) o 5 (se notificaron incidentes generalizados de explotación en diversas fuentes y las explotaciones son fáciles de lograr).

Además, las amenazas y explotaciones son más limitadas en su alcance frente a las explotaciones generalizadas consistentes en gusanos de Internet y código malicioso. Las amenazas suelen asociarse con kits de herramientas, que facilitan el inicio de los ataques mediante las vulnerabilidades individuales de cada sistema.

Según el Informe Anual de Seguridad de Cisco 2010, los grandes botnets como Zeus, que tuvo bajo su mando de 2 a 3 millones de computadoras en todo el mundo, se han utilizado para robar información bancaria y datos de acceso durante años. Recientemente, los creadores de botnets lanzaron kits de herramientas de ataque, en que el código del botnet está integrado, lo que permite crear una infinidad de botnets más pequeños.

Actualmente, los pocos botnets muy grandes, habitualmente administrados por empresas criminales afianzadas, fueron reemplazados por decenas de botnets más pequeños que se dedican a la actividad delictiva. "Cuando solo existían pocos botnets grandes, era más fácil vigilarlos y comprender cómo funcionaban", explicó Jeff Shipley, gerente de Investigación y Operaciones de Seguridad de Cisco. "La disponibilidad de los kits de herramientas de botnets aumentó mucho la cantidad de botnets, permite más variaciones y complica la tarea de analizar los patrones de comportamiento y brindar protección contra ellos".

Los nuevos botnets más pequeños siguen teniendo como blanco la información de cuentas bancarias, al igual que los botnets Zeus más grandes. Sin embargo, por la cantidad y variedad de estos botnets más pequeños a los profesionales de seguridad les resulta difícil seguir sus movimientos.

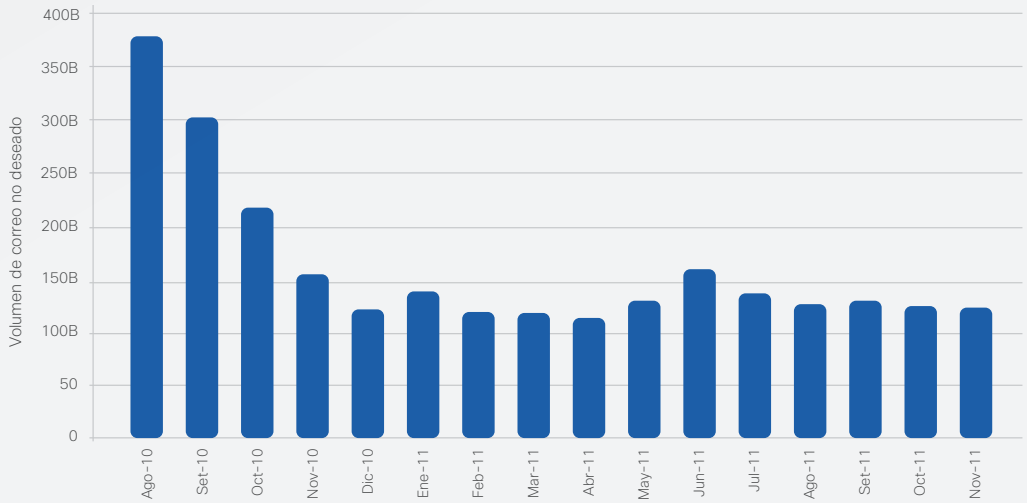
Actualización sobre correo no deseado a nivel mundial: Disminución radical del volumen de correo no deseado

Gracias a la preferencia de los delincuentes por las campañas dirigidas, el correo no deseado no parece ser tan lucrativo como solía ser. Según Cisco Security Intelligence Operations (SIO), el volumen de correo no deseado disminuyó de más de 300 mil millones de mensajes por día a menos de 40 mil millones de mensajes por día entre junio de 2010 y septiembre de 2011, niveles no observados desde 2006.

Antes de 2011, algunos ciberdelincuentes ya habían comenzado a cambiar su foco a ataques más dirigidos, utilizando sus recursos para llegar a personas específicas de una organización (como los empleados de los departamentos de finanzas o TI) mediante un mensaje fraudulento diseñado para obtener datos confidenciales de acceso a la red u otra información sobre cuentas. Basta una sola respuesta a las estafas dirigidas para que se las considere exitosas, mientras que las campañas masivas de correo no deseado exigen una tasa de respuesta mucho mayor para ser rentables.

Sin embargo, los acontecimientos observados durante el año pasado han alterado los modelos de negocio de los spammers tradicionales de manera tan notable que muchos se vieron obligados a canalizar sus recursos para desarrollar ataques dirigidos. A partir de 2010 y durante 2011, las autoridades de las fuerzas del orden, y las organizaciones de seguridad de todo el mundo trabajaron en estrecha cooperación para detener o limitar en gran medida la actividad de algunos de los botnets más grandes que envían correo no deseado. Spamlt, una red de afiliadas de envío de correo no deseado de gran magnitud, cerró en 2010 después de la que la policía rusa presentó cargos contra su propietario. Además, los principales botnets sufrieron limitaciones o se cerraron, como Rustock, Bredolab y Mega-D.

El impacto en el negocio del ciberdelito es importante: Según estimaciones de Cisco SIO, los beneficios cibercriminales derivados de los ataques tradicionales masivos de correo electrónico disminuyeron más del 50% (por año) entre junio de 2010 y junio de 2011, de mil cien millones de dólares a quinientos millones de dólares.[32]



Fuente: Cisco SIO

[32] *Email Attacks: This Time It's Personal*, Cisco, June 2011, www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.

Volumen de correo no deseado por país: Aspectos destacados de 2011

Cisco SIO también observa el volumen de mensajes de correo no deseado que se origina en todos los países del mundo. A septiembre de 2011, India tenía el máximo porcentaje de volumen de correo no deseado (13,9%). En 2010, el país ocupó el segundo lugar en volumen de correo no deseado, detrás de los Estados Unidos, que experimentó una disminución radical del volumen de correo no deseado entre enero y septiembre de 2011, del 10,1% al 3,2%. Hoy ocupa el noveno lugar en el volumen total de correo no deseado a nivel mundial.

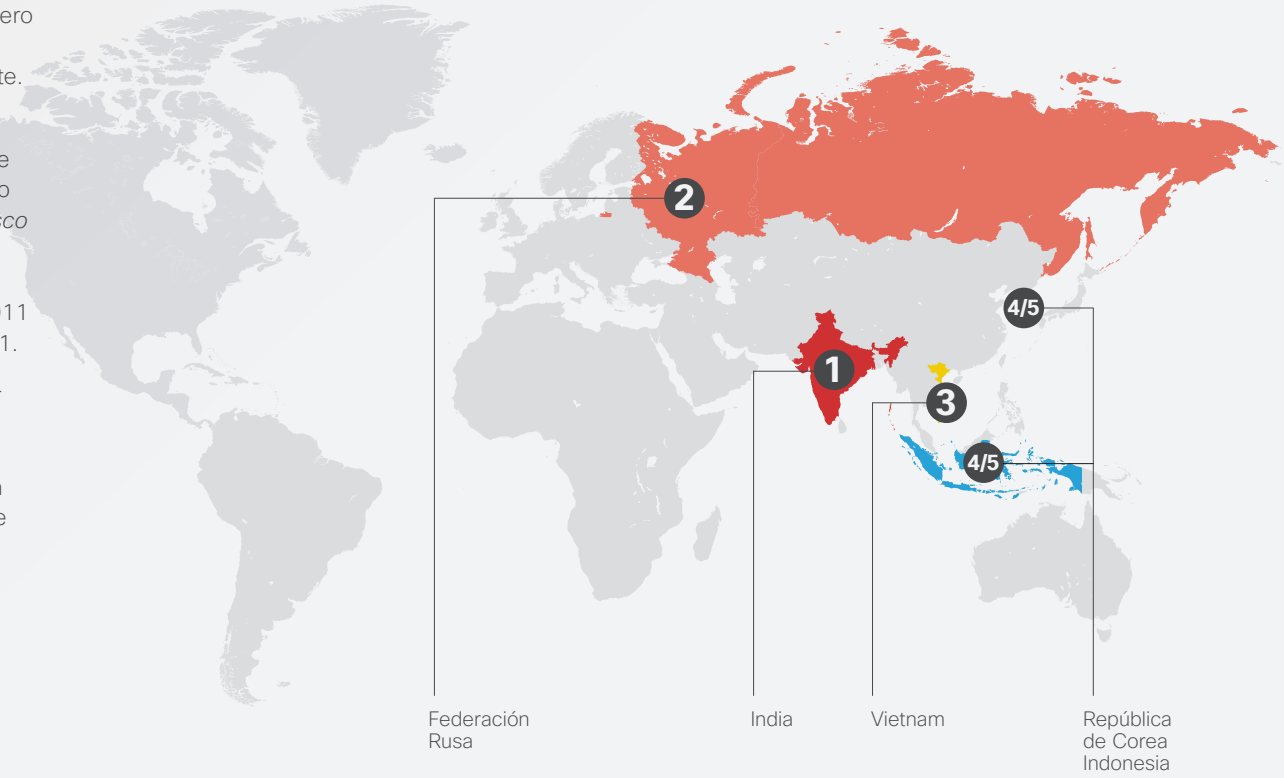
La Federación Rusa ocupó el segundo lugar en la lista de volumen de correo no deseado de este año, con un 7,8%. Su volumen de correo no deseado aumentó durante el primer semestre de 2011, del 7,6% en enero a un máximo del 9% en mayo; sin embargo, desde entonces viene registrando una disminución constante.

Vietnam ocupa el tercer lugar en la lista de 2011 y como la India y la Federación Rusa, se encontró entre los cinco principales países por su volumen de correo no deseado en el Informe *Anual de Seguridad de Cisco 2010*. El volumen de correo no deseado de Vietnam osciló entre el 3 y el 4% durante gran parte del año; sin embargo, aumentó a casi un 6% en agosto de 2011 y volvió a aumentar a casi 8% en septiembre de 2011.

Completan la lista de los cinco principales países por su volumen de correo no deseado la República de Corea e Indonesia, cada uno con un volumen total de correo no deseado del 6%, según la investigación de Cisco SIO. Ninguno de esos países apareció entre los 12 principales países por su volumen de correo no deseado en el informe del año pasado.

China, que ocupó el séptimo lugar en la lista de 2010, mantiene la misma posición en el ranking de este año. No obstante, si bien el volumen de correo no deseado de ese país ha registrado solo un ligero aumento general del 3,6% en diciembre de 2010 a un 4,7% en septiembre de 2011, fue el país con el máximo volumen de correo no deseado durante un breve período este año. Entre mayo y junio, el volumen total de correo no deseado de China aumentó del 1,1 a más del 10%. Su volumen de correo no deseado alcanzó un pico del 18% en julio y luego descendió a un 11,5% en agosto hasta disminuir de forma radical al 4,7% en septiembre.

Según la investigación de Cisco SIO, Brasil registró un volumen de correo no deseado en el orden del 4,5% en septiembre de 2011. Hoy, Brasil ocupa el octavo lugar entre los principales países por volumen de correo no deseado, después de haber ocupado los primeros puestos de la lista en 2009 y el tercer lugar en la lista del año pasado. Sin embargo, los volúmenes de correo no deseado del país ciertamente fluctuaron a lo largo de 2011, alcanzando un 8% en abril de 2011 hasta que comenzó un disminución constante a un 4,5%.



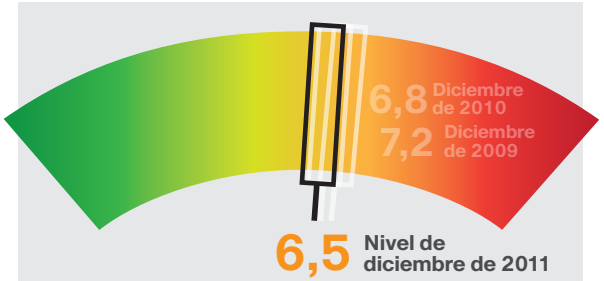
El Índice Cisco Global ARMS Race

El índice anual Cisco Global ARMS Race, que se basa en la escala de Richter utilizada para medir la magnitud de los terremotos, realiza el seguimiento de la "participación de mercado de los recursos del adversario" (Adversary Resource Market Share/ARMS). El índice sirve de instrumento para calcular el nivel general de recursos comprometidos en todo el mundo, las redes y máquinas que actualmente están bajo el "control del adversario". Los especialistas en seguridad de Cisco crearon el índice a fin de comprender mejor las tendencias globales en función de las actividades de la comunidad delictiva en línea a nivel mundial y sus tasas de éxito al comprometer a usuarios empresariales y particulares.

Según los datos recopilados para el índice de este año, la cantidad total que representa el nivel de recursos comprometidos a fines de 2010 es de 6,5, nivel ligeramente inferior al de 6,8 de diciembre de 2010. Cuando se presentó el Índice Cisco Global ARMS Race en el *Informe Anual de Seguridad de Cisco 2009*, la cantidad total fue de 7,2, es decir que las redes empresariales en ese momento estaban experimentando infecciones persistentes y los sistemas de consumo se infectaban a niveles con capacidad para producir niveles sistemáticos y alarmantes de abuso del servicio.

Desde entonces, los sistemas de consumo y empresas han experimentado una disminución constante de la tasa de infección; sin embargo, siguen manteniendo su "capacidad para producir niveles sistemáticos y alarmantes de abuso del servicio" y su "capacidad para provocar un amplio abuso del servicio de alto nivel (aunque no sostenido)". Lamentablemente, la magnitud de la disminución no cuenta toda la historia, puesto que cada copia de un programa malicioso APT de un delincuente provoca mucho más daño que en años anteriores.

¿Qué hay detrás de la disminución de este año en el nivel de recursos comprometidos a escala mundial? La disminución de la cantidad de botnets masivos impulsada por la intervención de las fuerzas del orden y los cierres de botnets ha tenido un impacto importante. Tal como se comentó antes en este informe, las operaciones delictivas sofisticadas se están distanciando de los botnets masivos, que eran comunes en años anteriores, porque las autoridades de las fuerzas del orden y el sector de seguridad mantienen una estrecha vigilancia de esta actividad. Sin embargo, se han desarrollado muchos botnets más pequeños. Cada uno de ellos tiene capacidad para provocar más daño por bot.



9,5+: Es mayor la cantidad de recursos que están bajo un control dudoso que uno legítimo. Incapacidad de confiar en cualquier conexión o aplicación, todos los servicios son susceptibles de denegación con facilidad.

9-9,5: Casi todas las redes, todos los tipos de máquinas, todos los tipos de usuario en todas las regiones sufren infecciones a niveles considerables. Es común el abuso de recursos.

8: Las redes empresariales sufren vastas infecciones de forma continua. Los sistemas de consumo sufren infecciones de gran magnitud y los programas tradicionales de seguridad no resultan ser eficaces. Son posibles los ataques simultáneos de envergadura en muchos objetivos de alta visibilidad.

7: Las redes empresariales experimentan infecciones persistentes. Los sistemas de consumo sufren infecciones a niveles capaces de producir niveles sistemáticos y alarmantes de abuso del servicio.

6: Las redes empresariales sufren infecciones con poca frecuencia. Los sistemas de consumo sufren niveles importantes de infecciones y tienen capacidad para producir un abuso del servicio amplio de alto nivel (aunque no sostenido).

5: Las redes empresariales rara vez sufren infecciones. Los sistemas de consumo experimentan infecciones molestas pero no alarmantes; el abuso dirigido de servicios es posible.

1-4: Las redes empresariales prácticamente no sufren infecciones. Los consumidores se enfrentan a niveles simbólicos de infecciones y el abuso es apenas perceptible.

Según el índice Cisco Global ARMS Race, el nivel de recursos bajo control del adversario a nivel mundial fue de 6,5 a fines de 2011. Se trata de una disminución del nivel de 6,8 de 2010, lo que demuestra que las infecciones de las redes empresariales y los sistemas de consumo son menos frecuentes en comparación con las registradas hace 12 meses.

Asimismo, muchos actores de la economía clandestina hoy centran sus esfuerzos en infectar objetivos específicos de alto valor con APT y lanzan ataques dirigidos que, sin duda, ofrecen un rendimiento lucrativo. La prevalencia de software malicioso con funciones completas para el robo de datos como Zeus y SpyEye ha permitido a muchas bandas delictivas lanzar ese tipo de ataques. "Las bandas de 'La Gran Estafa' andan por ahí", señaló Patrick Peterson, investigador senior de seguridad de Cisco. "Dedican mucha energía para comprometer una pequeña cantidad de objetivos de alto valor y no usan las técnicas de bombardeo de arrasamiento del pasado".

Methodología

Para llegar a la medición de este año del índice de diez puntos, Cisco se basó en las principales investigaciones de seguimiento de botnets del total de bots y otros datos obtenidos en investigaciones internas y otras fuentes especializadas, como The Shadowserver Foundation, que estudia la actividad cibercriminal y está integrada por profesionales de la seguridad voluntarios procedentes de todo el mundo. La metodología del índice Global ARMS Race se basa en:

- **Magnitud total actual de botnets**
- **Estadísticas utilizadas para estimar la cantidad total de sistemas conectados a Internet en el mundo**
- **Estimaciones de tasas de infección a nivel doméstico y laboral, que miden la disponibilidad de recursos, entre otros factores**

Internet: ¿Una necesidad humana fundamental?

El año 2011 fue testigo de nuevas y potentes maneras de usar Internet, en especial, para reunir a personas a una escala masiva para generar el cambio que ha modificado el panorama de nuestra comunidad mundial. Su influencia en nuestra vida cotidiana, tanto laboral como personal, también está aumentando. Por ende, cabe formular la siguiente pregunta: Si dependemos de Internet y su poder para conectarnos con información y personas de cualquier lugar del mundo, ¿es hoy una necesidad humana fundamental?

Según uno de cada tres estudiantes universitarios y jóvenes profesionales encuestados para el estudio de Cisco Connected World, sí lo es. De hecho, consideran que Internet es tan importante para su vida como el aire, el agua, la alimentación y la vivienda. Para algunos, esta actitud puede parecer extrema; sin embargo, no cabe duda de que es una posición que será común entre quienes integren la fuerza laboral de próxima generación. Si bien hoy observamos cómo se esfuma la línea divisoria entre el uso personal y profesional de Internet y las herramientas y tecnologías Web 2.0, pronto esa línea divisoria desaparecerá.

Mientras tanto, no existe ninguna duda de que para las empresas actuales, Internet es una necesidad para sus operaciones básicas y para aumentar su competitividad. Por esa razón solamente, parecería que en la empresa no se discutiría que debe adoptarse cualquier tecnología que aumente de forma considerable la productividad, eficiencia e innovación, y el nivel de satisfacción de los empleados, y que debe usarse esa tecnología de forma estratégica en toda la organización. Sin embargo, a muchas empresas les resulta difícil adaptarse a tantos cambios con tanta rapidez. Señalan que los problemas de seguridad son el principal obstáculo para aprovechar las nuevas tecnologías. Pero muchas están comenzando a comprender que una actitud expectante, si bien destinada a proteger a la empresa y sus recursos, puede en realidad socavar su competitividad si no ahora, sin duda, en el futuro.

Si las empresas avanzan muy lentamente no solo perderán la oportunidad de aprovechar las innovaciones que pueden permitirles lograr nuevos niveles de éxito, sino que tampoco podrán atraer ni retener a su recurso más importante: Los talentos. Como se mencionó en este informe, muchos de los empleados actuales preferirían no aceptar un puesto de trabajo si el posible empleador les dijera que sería muy limitado o se prohibiría su acceso a las redes y aplicaciones empresariales. (Consulte “Acceso remoto y estrategia BYOD: Empresas que trabajan para encontrar puntos en común con los empleados” en la página 10.)

De igual modo, más de la mitad de los estudiantes universitarios encuestados para el estudio Connected World señalaron que si encontraban una empresa que prohibía el acceso a los medios sociales, no aceptarían el empleo en esa organización o lo aceptarían pero tratarían de encontrar la manera de acceder a los medios sociales pese a las políticas de la empresa (consulte “Medios sociales: hoy, una herramienta de productividad” en la página 8).

Con todo, muchas empresas están tratando de cambiar. Los especialistas en seguridad de Cisco entrevistados para el Informe Anual de Seguridad de 2011 señalaron que muchas empresas están avanzando para desarrollar su modelo de seguridad de manera que resulte pertinente para el actual mundo conectado, y para tratar de encontrar puntos en común con los empleados que exigen el acceso a las aplicaciones y los dispositivos que desean utilizar para trabajar. Las empresas también están evaluando de nuevo sus políticas de uso aceptable y sus códigos de conducta empresarial, renovando sus iniciativas de prevención de pérdida de datos y conduciendo el debate sobre la seguridad de la empresa, y la responsabilidad de mantener los niveles deseados de seguridad, más allá de la función de TI a los departamentos de toda la organización, desde marketing, recursos humanos y legales hasta el nivel de la dirección.

Como se indica en este informe, Cisco es una de esas empresas. Al igual que numerosas organizaciones de todo el mundo, trabaja para lograr el equilibrio adecuado entre aprovechar nuevas oportunidades y mantener la seguridad de la red y los datos. La iniciativa “Cualquier Dispositivo” de Cisco, creada para permitir que los empleados de la compañía dispongan de más opciones en dispositivos y mantener una experiencia del usuario común y predecible que conserva o aumenta la competitividad y seguridad de la organización a escala mundial, es un importante punto de partida. Sin embargo, puede ser todo un desafío sentar las bases para adoptar un modelo BYOD.

> “La rápida erosión de este perímetro que se logró construir en 20 años deja a muchas empresas perplejas y con una sensación de vulnerabilidad cuando emprenden la transición a BYOD”.
>
> –Ofer Elzam, arquitecto de soluciones de seguridad integrada de Cisco

"Los smartphones y tablets modernos suponen una enorme revolución para TI", explicó Ofer Elzam, arquitecto de soluciones de seguridad integrada de Cisco. "Las empresas están condicionadas a mantener un perímetro de seguridad definido y a proteger ferozmente lo que se encuentra dentro de ella. La rápida erosión de este perímetro que se logró construir en 20 años deja a muchas empresas perplejas y con una sensación de vulnerabilidad cuando emprenden la transición a BYOD.

Desde varios puntos de vista, su sensación de vulnerabilidad es justificada. Si bien vivimos en un mundo conectado y ello supone que estamos más cerca de nuestros colegas, partners empresariales, clientes, amigos y familiares, nosotros y las organizaciones en las que trabajamos y con las que hacemos negocios también somos blancos más fáciles de la economía criminal. El carácter abierto e interconectado de los dispositivos móviles, las redes sociales y las aplicaciones Web 2.0 brinda nuevas alternativas a los actores maliciosos para robar a otros, alterar actividades comerciales o simplemente para manifestarse.

Los ciberdelincuentes está invirtiendo más en "I+D" para encontrar maneras de usar los dispositivos móviles y penetrar la nube a fin de apropiarse de los datos que necesitan con fines lucrativos o para socavar el éxito de una empresa. Además, como lo indica con claridad la tendencia al ciberactivismo pirata, hoy la tecnología permite a los revolucionarios sociales y delincuentes con ideas afines conectarse y reunirse de forma rápida, anónima e impredecible para lograr un objetivo específico que puede no estar motivado por el lucro o tener una finalidad que a otros, incluidos los objetivos, resulta fácil descifrar. "Algunas de las cosas que observamos el año pasado no se parecen a nada que hayamos visto antes", señaló Gavin Reid, gerente de CSIRT de Cisco. "Algunos acontecimientos fueron totalmente demoledores y esto no es una buena señal".

Como en nuestro propio planeta, el mundo conectado siempre tiene un lado iluminado y un lado oscuro. La seguridad de la empresa puede existir aquí; no obstante, para desarrollar un modelo eficaz es necesario generar nuevas ideas y aceptar algunos riesgos; además, su mantenimiento exige más vigilancia que nunca. Hoy en día, el principal desafío para las empresas es que deben encontrar la combinación adecuada de tecnología y política para satisfacer su combinación de necesidades particulares. No se trata de un proceso fácil, pero el resultado final será una empresa más dinámica y mejor preparada para adaptarse de manera rápida y segura a los cambios en la tecnología que inevitablemente se producirán en el futuro.

"El mundo conectado es un universo más fluido. Y, literalmente, ha llegado el momento de hundirse o salir a flote para las empresas que todavía tienen que aceptar que el cambio ya no está llamando a la puerta; por el contrario, ya está en su lugar de trabajo", explicó Chris Young, vicepresidente senior del Grupo de Seguridad de Cisco. "Al adoptar las tecnologías que sus empleados y sus clientes inevitablemente utilizarán, las empresas podrán crear una solución global de seguridad abordando la realidad y no preguntándose sobre situaciones hipotéticas".

Medidas a adoptar en 2012 para garantizar la seguridad de la empresa

Si bien las organizaciones deben desarrollar un enfoque de la seguridad de la red y los datos que satisfaga las necesidades específicas de su fuerza laboral y les permita lograr sus principales objetivos comerciales, existen varias cosas que cualquier empresa puede hacer para mejorar su posición de seguridad de inmediato y en el largo plazo. A continuación se ofrecen diez recomendaciones de los especialistas en seguridad de Cisco:

1 Evalúe la totalidad de la red. "Sepa dónde comienza y termina su infraestructura de TI. Demasiadas empresas no tienen idea de la totalidad de su red. También reconozca qué es 'normal' en su organización para poder identificar y responder a un problema con rapidez".

John N. Stewart, vicepresidente y director de seguridad de Cisco

2 Vuelva a evaluar la política de uso aceptable y el código de conducta empresarial. "Evite el enfoque de una larga lista cuando se trata de políticas de seguridad. Concéntrese únicamente en aquellas cosas que sabe que debe y puede implementar".

Gavin Reid, gerente de CSIRT de Cisco

3 Determine cuáles son los datos cuya protección es imprescindible. "No se puede desarrollar un programa eficaz de prevención de pérdida de datos si no se sabe qué información de la empresa debe protegerse. También debe determinarse quién en la empresa está autorizado a tener acceso a esa información y cómo podrá acceder a ella".

David Paschich, gerente de productos de seguridad web de Cisco

4 Sepa dónde están los datos y comprenda cómo (y si) están protegidos. "Identifique a todos los terceros que tienen permiso para almacenar datos de su empresa, desde proveedores de servicios en la nube hasta empresas de marketing por correo electrónico, y corrobore que se protege adecuadamente la información. Ante las obligaciones derivadas de la normativa vigente y ahora la tendencia en la ciberdelincuencia a "hackear a uno para hackear a todos", las empresas nunca deben suponer que los datos están protegidos, aunque los pongan en las manos de personas en quienes confían".

Scott Olechowski, gerente de investigaciones sobre amenazas de Cisco

5 Evalúe las prácticas de capacitación del usuario. "Los seminarios y manuales largos no son eficaces. Los empleados más jóvenes serán más receptivos a una estrategia específica de capacitación del usuario con sesiones más breves y capacitación 'justo a tiempo'. Por otra parte, la capacitación entre pares funciona bien en el entorno laboral de colaboración de hoy".

David Evans, futurista en jefe de Cisco

6 Utilice la supervisión de salida. "Esto es algo básico, pero no muchas empresas lo hacen, aunque por las exigencias normativas han aumentado las organizaciones que están adoptando esta práctica. La supervisión de salida es un cambio de enfoque que supone apartarse de la mera limitación de que entren 'los malos'. En rigor, se supervisa lo que sale de la organización, quién y a dónde, y se evita que salgan aquellas cosas que no deben salir".

Jeff Shipley, gerente de Investigación y Operaciones de Seguridad de Cisco

7 Prepárese para la inevitabilidad de BYOD. "Las organizaciones tienen que dejar de pensar en cuándo van a adoptar un modelo BYOD y comenzar a pensar más en *cómo*".

Nasrin Rezai, director senior de arquitectura y director de seguridad del Grupo Empresarial de Colaboración de Cisco

8 Elabore un plan de respuesta a incidentes. "El riesgo vinculado con la TI debe considerarse como cualquier otro riesgo empresarial. Por tanto, las empresas deben tener un plan claro para responder de forma rápida y adecuada a cualquier tipo de incidente de seguridad, ya sea una violación de datos producto de un ataque dirigido, una violación de cumplimiento a causa de la negligencia de un empleado o un incidente del ciberactivismo pirata".

Pat Calhoun, vicepresidente y gerente general de la Unidad de Negocio de Servicios de Redes Seguras de Cisco

9 Implemente medidas de seguridad para ayuda a compensar la falta de control sobre las redes sociales. "No subestime el poder de los controles tecnológicos, como un sistema de prevención de intrusiones, para brindar protección contra las amenazas a la red. El filtrado basado en la reputación es también una herramienta imprescindible para detectar actividades y contenidos sospechosos".

Rajneesh Chopra, director de administración de productos, Grupo de Tecnología de Seguridad de Cisco

10 Supervise el panorama de riesgos dinámico y mantenga informados a los usuarios. "Las empresas y sus equipos de seguridad deben vigilar una gama mucho más amplia de fuentes de riesgo, desde dispositivos móviles y la nube hasta las redes sociales y lo que sea que incorpore la nueva tecnología en el futuro. Deben adoptar una estrategia de dos etapas: Reaccionar ante las divulgaciones de vulnerabilidad de seguridad y ser proactivo en capacitar a sus empleados sobre su protección y la de la empresa contra las amenazas cibernéticas persistentes y potentes".

Ofer Elzam, arquitecto de soluciones de seguridad integrada de Cisco

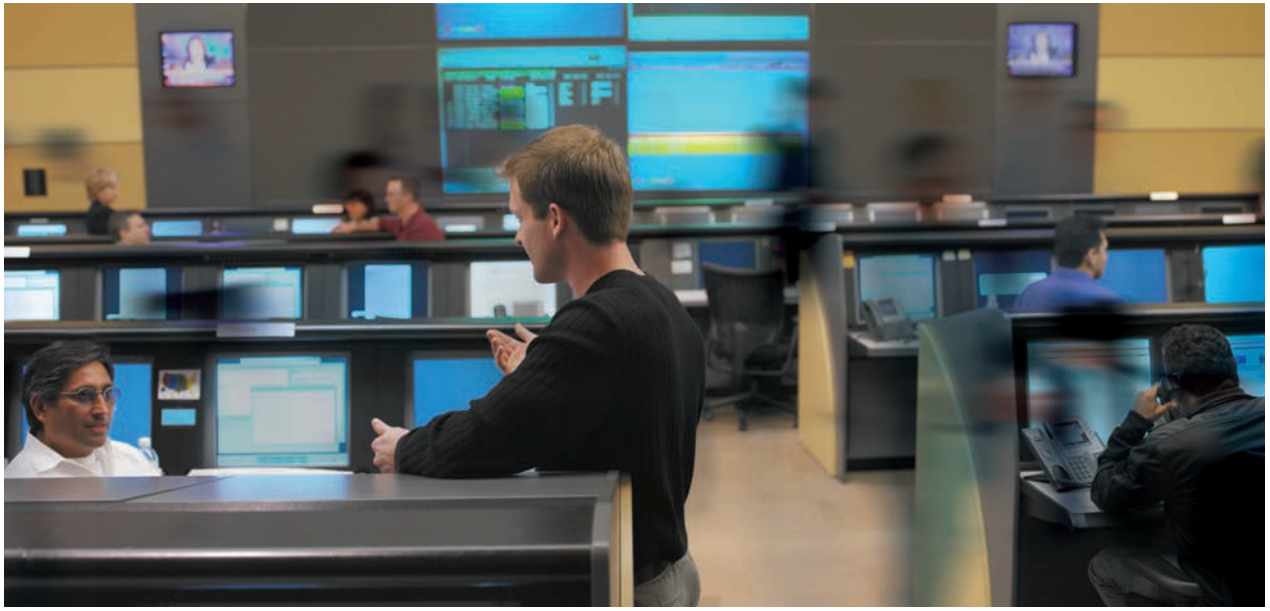
Inteligencia sobre seguridad de Cisco

Es un desafío mayúsculo administrar y proteger las redes distribuidas y dinámicas de la actualidad. Los delincuentes en línea se siguen aprovechando de la confianza de los usuarios en aplicaciones y dispositivos de consumo, lo que aumenta el riesgo para las organizaciones y los empleados. La seguridad tradicional, que se basa en la distribución en capas de productos y el uso de varios filtros, ya no basta como defensa contra la generación más reciente de software malicioso, que se propaga con rapidez, tiene blancos a nivel mundial y utiliza varios vectores para su propagación.

Cisco se mantiene un paso adelante de las amenazas más recientes mediante la inteligencia sobre amenazas en tiempo real de Cisco Security Intelligence Operations (SIO). Cisco SIO es el ecosistema más grande del mundo de seguridad basado en la nube, que utiliza los datos de SensorBase de casi un millón de fuentes de datos en vivo procedentes de las soluciones Cisco para correo electrónico, de firewall y el sistema de prevención de intrusiones (IPS).

Cisco SIO pondera y procesa los datos, categoriza de forma automática las amenazas y crea reglas con más de 200 parámetros. Los investigadores de seguridad también recopilan y suministran información sobre incidentes de seguridad que pueden tener un impacto generalizado sobre redes, aplicaciones y dispositivos. Las reglas se distribuyen de forma dinámica entre los dispositivos de seguridad Cisco cada tres o cinco minutos. El equipo de Cisco SIO también publica recomendaciones de mejores prácticas de seguridad y guías tácticas para combatir las amenazas.

Cisco ha asumido el compromiso de proporcionar soluciones de seguridad completas, integradas, oportunas y eficaces, que permiten adoptar una estrategia holística de seguridad en las organizaciones de todo el mundo. Con Cisco, las organizaciones pueden ahorrar el tiempo que usan para investigar amenazas y vulnerabilidades, y concentrarse más en la adopción de un enfoque proactivo de la seguridad



El **servicio Cisco Security IntelliShield Alert Manager** ofrece una solución completa y económica para brindar la inteligencia sobre seguridad independiente del proveedor que las organizaciones necesitan para identificar, evitar y mitigar los ataques contra la TI. Este servicio personalizable de alerta de amenazas y vulnerabilidades de la web permite al personal de seguridad tener acceso a información oportuna, precisa y confiable sobre las amenazas y vulnerabilidades que podrían afectar a sus entornos. IntelliShield Alert Manager permite a las organizaciones invertir menos esfuerzos en la investigación de amenazas y vulnerabilidades, y concentrarse más en un enfoque proactivo de la seguridad.

Cisco ofrece una evaluación de prueba gratuita durante 90 días del servicio Cisco Security IntelliShield Alert Manager. Al inscribirse en esta evaluación, tendrá total acceso al servicio, las herramientas y alertas de amenazas y vulnerabilidades.

Para obtener más información sobre los servicios Cisco Security Intellishield Alert Manager, visite: https://intellishield.cisco.com/security/alertmanager/trial.do?dispatch=4

Para obtener información de advertencias anticipadas, análisis de amenazas y vulnerabilidades y las soluciones de mitigación de Cisco de eficacia comprobada, visite: www.cisco.com/go/sio.

Arquitectura Cisco SecureX

La arquitectura Cisco SecureX es un marco con capacidad de reconocimiento del contexto de próxima generación que satisface las necesidades en evolución en materia de seguridad de entornos borderless network.

A diferencia de las arquitecturas de seguridad antiguas que se desarrollaron para implementar políticas basadas en un solo punto de datos, Cisco SecureX implementa las políticas en función de todo el contexto de la situación. Las políticas con capacidad de reconocimiento del contexto utilizan un lenguaje de alto nivel que se alinea estrechamente con la política empresarial. Así se simplifica en gran medida la administración de política y al mismo tiempo se ofrece seguridad y control más eficaces. En consecuencia, las redes son mucho más seguras, al tiempo que se maximizan la eficiencia y flexibilidad de la empresa.

La arquitectura Cisco SecureX:

Implementa políticas con capacidad de reconocimiento del contexto en una amplia gama de formatos para proporcionar seguridad de forma flexible, en el momento y lugar en que se necesite.

Administra las políticas de seguridad con capacidad de reconocimiento del contexto en toda la red, lo que facilita información profunda y controles eficaces respecto de quién está haciendo qué, cuándo, dónde y cómo.

Proporciona un acceso seguro desde una gama completa de dispositivo, desde PC tradicionales hasta computadoras Mac, smartphones, tablets y otros dispositivos móviles, en cualquier momento y lugar.

Aprovecha los aportes de SIO para contar con sólida información en tiempo real del entorno de amenazas a escala mundial.

Permite simplificar las políticas empresariales que se correlacionarán directamente entre lo que el departamento de TI debe implementar y las normas comerciales de la organización.

Integra API completas y ampliables que permiten que sistemas de administración propia y partners de Cisco se conecten y completen el ecosistema de seguridad.

Para obtener más información sobre la arquitectura Cisco SecureX, visite www.cisco.com/en/US/netsol/ns1167/index.html.

Para obtener más información

Cisco Security Intelligence Operations
www.cisco.com/security

Blog de Cisco sobre seguridad
blogs.cisco.com/security

Cisco Remote Management Services
www.cisco.com/en/US/products/ps6192/serv_category_home

Productos de seguridad de Cisco
www.cisco.com/go/security

Cisco Remote Management Services
www.cisco.com/go/cspo

El informe puede descargarse de
www.cisco.com/go/securityreport

Sede en América
Cisco Systems, Inc.
San Jose, CA

Sede en la región Asia-Pacífico
Cisco Systems (USA) Pte. Ltd.
Singapur

Sede en Europa
Cisco Systems International BV Amsterdam,
Holanda

Cisco cuenta con más de 200 oficinas en todo el mundo. Puede encontrar las direcciones, números de teléfono y de fax en el sitio web de Cisco en la dirección www.cisco.com/go/offices.