EMPRESAS SEGURAS

Tecnologías y estrategias que le permitirán mantener su negocio en marcha sin problemas

kaspersky.com/enterprise
#EnterpriseSec

KASPERSKY lab

EL PODER DE LA PROTECCIÓN

Eugene Kaspersky
Director ejecutivo y presidente de Kaspersky Lab

PROTEGEMOS EL PRESENTE PARA ASEGURAR EL FUTURO

Todos los días, miles de millones de personas acceden y comparten información online. Se produce un trasiego incesante de datos entre empresas, empleados, clientes y proveedores de todo el mundo.

Toda esta conectividad aporta inconmensurables beneficios comerciales, pero también plantea un riesgo considerable y cada vez mayor para la seguridad. Cada día aparecen nuevas ciberamenazas con potencial para causar efectos devastadores en las personas, las empresas y las sociedades.

Durante muchos años he estado trabajando estrechamente con organismos gubernamentales y fuerzas del orden de todo el mundo para ofrecer asesoramiento acerca de los peligros a los que nos enfrentamos y la importancia crucial de la ciberseguridad. Lamentablemente, las amenazas ganan en sofisticación a cada día que pasa. Para ver cómo evolucionan, no tenemos más que echar un vistazo a algunos de nuestros más recientes descubrimientos, incluidos Carbanak, Equation y Darkhotel.

Prevenir la ciberguerra y el ciberterrorismo ya ocupa un lugar prioritario en las agendas de los líderes de todo el mundo, mientras que en el caso de las empresas, ahora es el momento de volver a examinar sus estrategias de seguridad de IT para garantizar que satisfacen las exigencias de un entorno cada vez más complejo y problemático.

Como una empresa de servicios de seguridad, sabemos que responder a las nuevas amenazas a medida que aparecen no es suficiente. Por eso invertimos tantos recursos y esfuerzos en nuestra investigación de amenazas, una iniciativa líder a nivel mundial. Nunca dejamos de anticiparnos ni de prevenir amenazas de seguridad de IT, y nuestras tecnologías de protección en varios niveles están diseñadas para sacar el máximo partido a la amplia inteligencia de seguridad global con que contamos. Nuestro enfoque es sencillo: combinar una mejor inteligencia con mejor tecnología conlleva una mejor seguridad.

"ESTAMOS SIEMPRE PREPARADOS PARA COMBATIR EL CIBERCRIMEN INDEPENDIENTEMENTE DE SU ORIGEN, SU OBJETIVO Y SU GRADO DE SOFISTICACIÓN. LA EFICACIA DE NUESTRAS SOLUCIONES RESIDE EN LA FUSIÓN DE CAPACIDAD TECNOLÓGICA DEMOSTRADA Y DE LA INVESTIGACIÓN EN SEGURIDAD LÍDER EN EL MUNDO. ESTA COMBINACIÓN PRODUCE RESULTADOS SIN RIVAL EN NINGUNA OTRA EMPRESA DE SEGURIDAD DE IT".

Nikita Shvetsov
Director de tecnologías de la información
Kaspersky Lab

El malware afecta a todo el mundo, tanto si se trata de particulares como de grandes empresas o incluso organismos gubernamentales. Los cibercriminales están usando armas cada vez más sofisticadas para cometer fraudes contra empresas, robar datos y hacerse con cuantiosos beneficios financieros. El ciberterrorismo y la ciberguerra ya son una realidad y, si bien el número de ciberataques con motivación política o social va en aumento, los ciberterroristas y activistas hackers centran su atención en las empresas.

Las empresas globales están expuestas a ataques dirigidos, conocidos también como amenazas avanzadas persistentes o APT (del inglés "Advanced Persistent Threats"), por parte de grupos criminales específicos. Aunque algunos de estos casos reciben abundante cobertura en los medios, la tendencia entre los atacantes consiste en utilizar técnicas subrepticias para evitar que se detecte el ataque y, mientras, continúan teniendo acceso a datos delicados de gran valor comercial.

NUESTRA ESTRATEGIA

En Kaspersky Lab, la estrategia y el enfoque de I+D están localizados en el lugar mismo en el que se generan las amenazas emergentes, y en aquellos puntos en los que las organizaciones son más vulnerables.

Nuestro bagaje y nuestra experiencia se han centrado siempre en proteger los endpoints. Hoy en día, la gama de endpoints es más variada y pueden ser físicos, móviles y virtuales, o incluso formar parte de la infraestructura vital de un país, y todos ellos están más expuestos que nunca.

Ayudamos a las grandes empresas a proteger estas áreas vulnerables mediante un enfoque capaz de sacar partido a nuestra inteligencia avanzada contra amenazas para ofrecer un mayor nivel de protección.

LIDERAZGO TECNOLÓGICO

A pesar de su variedad, estas amenazas no existen de manera aislada. En su conjunto forman parte de un panorama de seguridad más amplio, y para vencer cualquiera de ellas es preciso entenderlas en su conjunto. En lugar de ofertas destinadas a un uso concreto, diseñadas con un enfoque limitado, las soluciones de seguridad deben crearse sobre la base de una inteligencia de seguridad extensa y predictiva.

Estamos convencidos de que para crear soluciones de seguridad eficaces, es necesario contar con una perspectiva lo más amplia posible. Este principio sirve de guía a nuestra estrategia tecnológica y tiene como resultado soluciones integradas creadas y diseñadas de forma orgánica, que ofrecen una protección superior y un mejor rendimiento. Como ya hemos señalado, una mejor inteligencia combinada con tecnología mejor se traduce en una mayor protección.

Un elemento clave de nuestra inteligencia en seguridad es Kaspersky Security Network (KSN). Dicha red recibe grandes cantidades de datos de ciberamenazas sobre todo tipo de malware en evolución procedentes de todos los confines del mundo. La combinación de estos datos y el análisis de nuestro renombrado equipo de análisis e investigación global (GReAT, del inglés "Global Research and Analysis Team") nos permite situarnos en una posición única para brindar soluciones que no solo neutralizan las amenazas actuales, sino que ayudan a luchar contra los peligros futuros. De esta forma, nuestros clientes se benefician de la protección contra las amenazas más recientes.

LA RED KASPERSKY SECURITY NETWORK

- Una infraestructura distribuida compleja dedicada a procesar flujos de datos desprovistos de información personal relacionados con ciberseguridad y procedentes de millones de participantes voluntarios repartidos por todo el mundo
- Con la participación de unos 60 millones de voluntarios
- 600 000 solicitudes de datos por segundo
- Respuesta media a una solicitud de un cliente: 0,02 segundos

EN UN PANORAMA EN EL QUE LOS ATAQUES SON CADA VEZ MÁS SOFISTICADOS Y TIENEN UNA MAYOR CAPACIDAD DE EVASIÓN, LA TECNOLOGÍA ANTIMALWARE Y LOS FIREWALLS CONVENCIONALES YA NO SON SUFICIENTES. SE NECESITAN HERRAMIENTAS QUE SE INTEGREN MÁS PROFUNDAMENTE Y MEJOR EN LA INFRAESTRUCTURA.

Los departamentos de IT de las grandes empresas se enfrentan a desafíos por partida doble: la complejidad de IT es cada vez mayor, y las amenazas son cada vez más sofisticadas. Para complicar todavía más la tarea del equipo de IT, la red corporativa habitual utiliza día a día un gran abanico de aplicaciones y dispositivos, y el número de empleados que realizan transacciones a través de la web y las plataformas de redes sociales aumenta continuamente.

Hoy en día, las empresas necesitan que la seguridad de IT sea más amplia y esté gestionada de un modo más preciso.

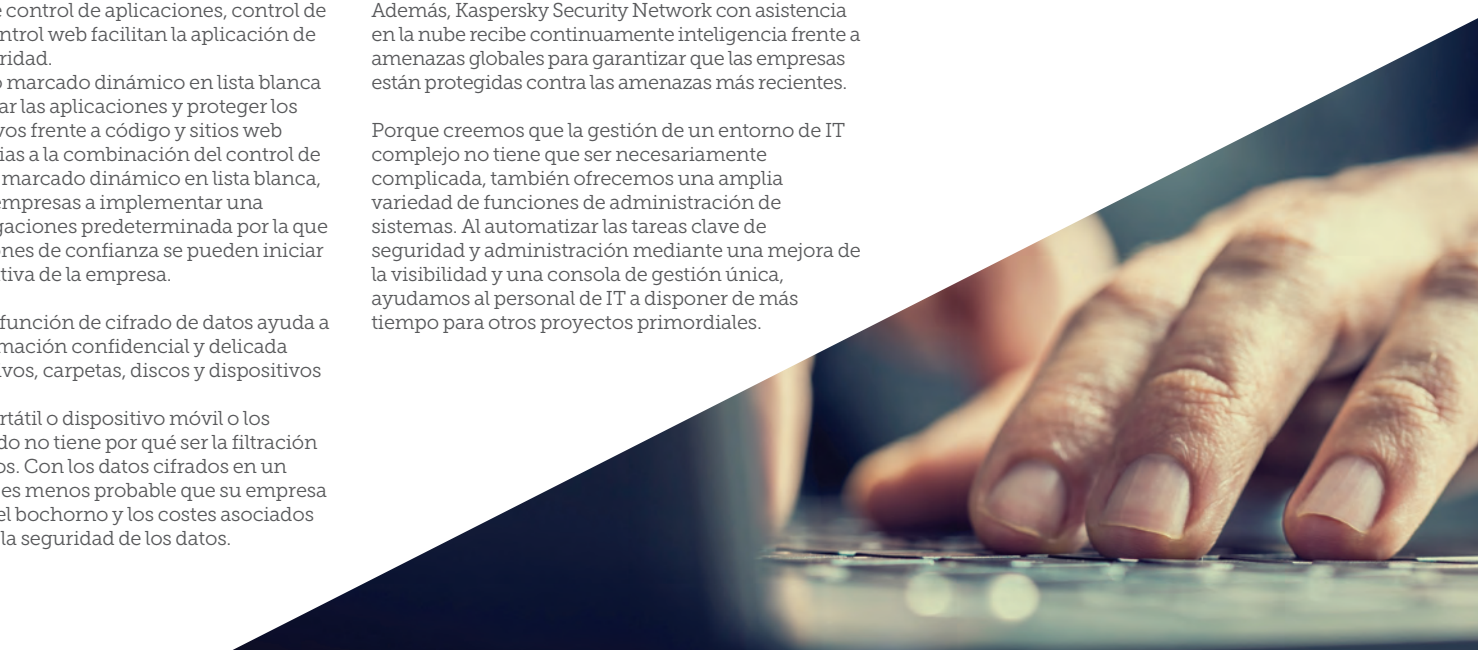
Las soluciones de seguridad para endpoints para empresas de Kaspersky Lab incorporan herramientas de control flexible, cifrado de datos y funciones de administración de sistemas.

Las funciones de control de aplicaciones, control de dispositivos y control web facilitan la aplicación de políticas de seguridad.
Además, nuestro marcado dinámico en lista blanca ayuda a autenticar las aplicaciones y proteger los datos y dispositivos frente a código y sitios web maliciosos. Gracias a la combinación del control de aplicaciones y el marcado dinámico en lista blanca, ayudamos a las empresas a implementar una política de denegaciones predeterminada por la que solo las aplicaciones de confianza se pueden iniciar en la red corporativa de la empresa.

Nuestra potente función de cifrado de datos ayuda a proteger la información confidencial y delicada incluida en archivos, carpetas, discos y dispositivos extraíbles.
Si le roban un portátil o dispositivo móvil o los pierde, el resultado no tiene por qué ser la filtración de datos delicados. Con los datos cifrados en un formato ilegible, es menos probable que su empresa tenga que sufrir el bochorno y los costes asociados con la brecha en la seguridad de los datos.

Además, Kaspersky Security Network con asistencia en la nube recibe continuamente inteligencia frente a amenazas globales para garantizar que las empresas están protegidas contra las amenazas más recientes.

Porque creemos que la gestión de un entorno de IT complejo no tiene que ser necesariamente complicada, también ofrecemos una amplia variedad de funciones de administración de sistemas. Al automatizar las tareas clave de seguridad y administración mediante una mejora de la visibilidad y una consola de gestión única, ayudamos al personal de IT a disponer de más tiempo para otros proyectos primordiales.



EL 94 % DE LAS EMPRESAS HA EXPERIMENTADO ALGUNA FORMA DE AMENAZA A LA SEGURIDAD EXTERNA.[1]

[1] Informe de riesgos de IT globales de 2014, Kaspersky Lab

EN LOS ÚLTIMOS CUATRO AÑOS, EL 30 % DE LAS EMPRESAS HAN SUFRIDO LA PÉRDIDA O EL ROBO DE UN DISPOSITIVO MÓVIL, Y SIGUE SIENDO LA SEGUNDA FORMA MÁS HABITUAL DE PÉRDIDA DE DATOS DE UNA EMPRESA.[3]

Con el auge de la flexibilidad laboral y las políticas de uso de dispositivos personales en el entorno de trabajo "traiga su propio dispositivo" o BYOD (del inglés "Bring Your Own Device"), las empresas necesitan garantizar que su solución de seguridad protege contra las ciberamenazas independientemente de si los usuarios se encuentran en la oficina o fuera.

La cantidad de malware destinada específicamente a los dispositivos móviles está creciendo de manera exponencial. Incluso una brecha puntual de seguridad en un teléfono o tablet puede comprometer la seguridad de toda una red corporativa. Ya se trate de un ataque inadvertido en una página web infectada visitada por el usuario, una aplicación maliciosa que ha descargado o la pérdida física de un dispositivo móvil, el daño puede ser considerable.

Además, la amplia variedad de tipos de dispositivos y la evidente la portabilidad de estos pueden aumentar considerablemente la carga de gestión de la seguridad.

Kaspersky Security for Mobile ofrece rigurosas tecnologías de seguridad, incluidos antimalware avanzado, control de aplicaciones y funciones antirrobo, para ayudar a proteger las redes corporativas y los datos de la empresa frente a una amplia variedad de amenazas móviles.

Una consola de gestión unificada ofrece a las empresas visibilidad y control centralizados de todas las tecnologías de seguridad para endpoints de Kaspersky Lab que se están ejecutando en los endpoints físicos, virtuales y móviles.

[2] http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/
[3] Informe de riesgos de IT globales de 2014, Kaspersky Lab

SOLUCIONES DE SEGURIDAD DE KASPERSKY PARA CENTROS DE DATOS
Protección de las tecnologías clave

LOS PRODUCTOS DE KASPERSKY LAB HAN DETECTADO Y NEUTRALIZADO UN TOTAL DE 6 167 233 068 AMENAZAS EN UN PERIODO DE 12 MESES.[4]

Casi todas las empresas se enfrentan a la necesidad de almacenar volúmenes de datos cada vez mayores, al mismo tiempo que se debe mantener el acceso a los datos y garantizar la seguridad.

Dos tecnologías clave son esenciales para incrementar la eficiencia del almacenamiento y la gestión de datos en los centros de datos: la virtualización y los sistemas de almacenamiento. No obstante, cuando se trata de amenazas a la seguridad, estas tecnologías son a menudo más vulnerables que cualquier otro componente de un centro de datos.

Ofrecemos soluciones que se centran en la protección de estos dos ámbitos esenciales de los centros de datos. Tenemos productos de seguridad adecuados para entornos con varios hipervisores y todos los sistemas de almacenamiento más conocidos:

- Seguridad especializada para las principales plataformas de virtualización, como VMware, Citrix y Microsoft
- Seguridad para sistemas de almacenamiento NAS y SAN, incluidos EMC, NetApp e Hitachi

Estas soluciones están diseñadas para ofrecer una seguridad completa que abarca la mayoría de los riesgos en los centros de datos de cualquier configuración, incluso aquellos que funcionan en nubes públicas, como Amazon o Microsoft Azure.

Por otra parte, como una mejora en la capacidad de gestión ayuda a reducir los costes y liberar valiosos recursos de IT para las iniciativas empresariales estratégicas, también proporcionamos una consola de gestión central que permite a los administradores controlar una amplia variedad de tareas, incluidas la instalación y configuración remotas, y la generación de informes para ambas soluciones de seguridad.

[4] Boletín de seguridad de Kaspersky 2014 (datos de Kaspersky Security Network)

A FINALES DE 2016, APROXIMADAMENTE EL 85 % DE LAS CARGAS DE TRABAJO DE SISTEMAS OPERATIVOS EN SERVIDORES X86 EN LAS INSTALACIONES ESTARÁN VIRTUALIZADAS.[5]

La virtualización ha transformado los entornos de IT grandes y complejos, reportando beneficios considerables a las empresas.

No obstante, con el crecimiento de las ciberamenazas, las empresas deben proteger sus entornos virtuales de forma tan plena y eficaz como protegen sus activos de IT físicos. Muchas empresas están ampliando ahora sus iniciativas de virtualización y están virtualizando sistemas críticos, por lo que incluso hay más en juego.

Añadir funciones de seguridad a cualquier sistema de IT, físico o virtual, va a ir asociado a un consumo de recursos. Así pues, nuestro objetivo constante es maximizar la protección y minimizar el impacto en los recursos. Este problema es particularmente crítico para la infraestructura virtual, ya que la eficiencia de los recursos es el impulsor principal para la implementación de la virtualización. A menos que se mantenga un equilibrio adecuado entre la seguridad y la eficiencia, muchas de las ventajas de la virtualización pueden quedar totalmente invalidadas.

Kaspersky Security for Virtualization se ha desarrollado específicamente para la seguridad de las máquinas virtuales. Al ofrecer seguridad que supone menos carga para los recursos informáticos, las empresas podrán mantener una alta densidad de virtualización y un alto rendimiento para aumentar el retorno de la inversión.

En lugar de tener que instalar un agente de seguridad de tamaño completo en cada una de las máquinas virtuales, Kaspersky Security for Virtualization ofrece una manera más eficaz de proteger los entornos virtualizados que ayuda a minimizar la carga en los procesadores, la memoria, el almacenamiento y E/S, a la vez que tiene en cuenta las necesidades específicas de los entornos virtuales.

[5] Gartner Forecast Overview: Enterprise Infrastructure Software, Worldwide (Descripción general de la previsión de Gartner: software de infraestructuras empresariales a escala mundial). Publicación: 15 de agosto de 2014

LOS ATAQUES DE DDOS EN EL 2º TRIMESTRE DE 2014 AUMENTARON EN UN 22 % EN COMPARACIÓN CON EL MISMO PERIODO DEL AÑO ANTERIOR.[6]

Los cibercriminales utilizan ataques de denegación de servicio distribuidos (DDoS, del inglés "Distributed Denial of Service") para desactivar la presencia online de una empresa o de sus procesos empresariales clave. Mientras que los costes financieros directos de un ataque de DDoS pueden ser enormes, las empresas víctimas también puede sufrir graves daños en lo que se refiere a su marca y reputación, sobre todo si los tiempos de inactividad de la infraestructura y los procesos críticos para la empresa afectan negativamente al servicio al cliente durante un periodo de tiempo prolongado.

En los últimos años, el coste de lanzamiento de un ataque de DDoS se ha reducido, por lo que se ha producido un crecimiento importante en el volumen de los ataques. Al mismo tiempo, muchos de los ataques se han vuelto mucho más sofisticados.

A diferencia de los ataques de malware que tienden a propagarse automáticamente, los ataques de DDoS sofisticados de la actualidad dependen de la experiencia humana, y esto puede hacer que los ataques de DDoS sean especialmente difíciles de combatir. Esto significa que la implementación de defensas diseñadas en torno a un enfoque basado en inteligencia es esencial.

La protección contra DDoS de Kaspersky ofrece una solución completa e integrada de protección y mitigación contra ataques DDoS que se ocupa de todas las fases necesarias para defender una empresa contra todos los tipos de ataques de DDoS. Nuestra solución incluye análisis ininterrumpido de todo el tráfico online de nuestros clientes, la emisión de alertas sobre la posible presencia de un ataque, la recepción del tráfico redirigido del cliente, la limpieza de dicho tráfico y la devolución del tráfico "limpio" a la empresa. Por otra parte, generamos informes y análisis posteriores al ataque.

Somos el primer proveedor antimalware que ofrece una solución de protección contra DDoS. Proporcionamos una combinación exclusiva de análisis estadístico, análisis de comportamiento e inteligencia de ataque de DDoS, por lo que podemos ofrecer una defensa más exhaustiva contra ataques de DDoS.

[6] Prolexic Quarterly Global DDOS Attack Report Q2 2014 (Informe trimestral sobre ataques de DDOS globales de Prolexic, segundo trimestre de 2014)

EN 2018, EL 40 % DE LAS GRANDES EMPRESAS DISPONDRÁN DE PLANES OFICIALES PARA ABORDAR LOS ATAQUES AGRESIVOS CONTRA LA CIBERSEGURIDAD A TRAVÉS DE LA INTERRUPCIÓN DEL NEGOCIO, CON UN 0 % EN 2015.[7]

Las empresas modernas tienen que procesar volúmenes de información en continuo aumento. Gran parte de los datos pueden ser delicados o tener gran un valor comercial, y los cibercriminales son plenamente conscientes de esto. Mediante el lanzamiento de amenazas avanzadas persistentes o APT (del inglés "Advanced Persistent Threats") contra un objetivo específico, los cibercriminales pueden robar información confidencial e incluso espiar a los empleados de una empresa.

Como las APT son mucho más complejas que elementos aislados de malware, son mucho más difíciles de detectar y bloquear. Cada ataque de APT está adaptado para lograr objetivos concretos contra una empresa objetivo específica, y por lo general incluirá varios procesos que llevan a cabo diferentes etapas del ataque. Normalmente, el atacante también deseará garantizar que la brecha en la seguridad siga sin detectarse, por lo que el robo de datos puede realizarse de manera continuada durante un periodo de tiempo prolongado.

Hace escasos años se llevaban a cabo pocos ataques de este tipo debido al alto coste del desarrollo de una APT. No obstante, el coste del lanzamiento de un ataque de APT se ha reducido a un nivel más bajo, por lo que los cibercriminales ahora consideran que las APT son una forma rentable de atacar a las empresas.

Debido a que el ingenio humano implicado en el diseño y la implementación de una APT juega un papel importante, la inteligencia de seguridad de gran calidad es un factor de vital importancia para derrotar con éxito estas amenazas.

Kaspersky Lab ha sido reconocido como el primer proveedor en detectar muchas de las APT más peligrosas del mundo, y consideramos la inteligencia de amenazas como la base fundamental para el diseño de tecnologías de protección eficientes para los endpoints y las redes. Creemos que la combinación de inteligencia y productos y servicios de seguridad permite la implementación de una estrategia contra APT potente en varios niveles que ayuda a bloquear las brechas de seguridad, identificar rápidamente cuándo se está produciendo un "ataque directo", bloquear las amenazas y distribuir análisis de ciencia forense posteriores al ataque.

[7] Gartner, Attack on Sony Pictures Is a Digital Business Game Changer (Gartner, El ataque a Sony Pictures cambiará las reglas del juego en el sector de los negocios digitales). Publicación: 9 de febrero de 2015

En el pasado, los sistemas de control industrial estaban aislados y el sector pensaba que esto era suficiente para mantener su infraestructura segura. En realidad, el aislamiento nunca ha sido una garantía suficiente de seguridad. Como se ha demostrado en los casos recientes de alto nivel, los ataques pueden originarse en cualquier parte, hasta el punto de que el control de una central nuclear puede sucumbir a malware introducido a través de un puerto USB.

Hoy en día, la necesidad de conectar sistemas a Internet introduce una gran variedad de nuevas vulnerabilidades en estos sistemas y, en el caso de que se produzca un ataque de malware a una red, las consecuencias pueden ser catastróficas.

A pesar de que muchas ciberarmas están diseñadas con objetivos específicos en mente, también pueden afectar a otras empresas. Después del lanzamiento de una nueva ciberarma, esta puede caer en las manos de un gran número de grupos con planes hostiles, y el arma se puede volver a configurar para atacar nuevos objetivos.

Una infraestructura vital necesita el nivel de protección más alto posible contra una variedad creciente de amenazas.

Como líder en la lucha contra el cibercrimen, Kaspersky Lab conoce como nadie las amenazas globales y, además, cuenta con la experiencia necesaria para combatirlas. En colaboración con gobiernos y organismos del sector privado, ayudamos a crear las defensas en varios niveles necesarias para proteger infraestructuras vitales. Reconocemos que las infraestructuras vitales necesitan un nivel de protección distinto.

En el caso de las redes industriales, la continuidad del proceso siempre tiene prioridad sobre la confidencialidad y la integridad de los datos. Somos líderes en el sector en lo que se refiere al desarrollo de soluciones de infraestructuras seguras, protección especializada para PLC (controladores lógicos programables) y niveles de protección SCADA más integrados.

EL 40 % DE LOS PROFESIONALES DE IT DEL SECTOR INDUSTRIAL NOTIFICARON BRECHAS IDENTIFICADAS O SOSPECHADAS, LO QUE REPRESENTA UN AUMENTO DEL 28 % CON RESPECTO A 2013.[8]

[8] SANS Institute: 2014 Control System Security Survey (SANS Institute: encuesta de seguridad de sistemas de control de 2014)
[9] Cyberthreats to ICS systems: you don't have to be a target to become a victim (Las ciberamenazas a los sistemas de control internacionales: no hace falta ser el objetivo para convertirse en la víctima).
Industrial Security 2014 (Seguridad industrial 2014), Kaspersky Lab

EL 73 % DE LAS EMPRESAS TIENE EN CUENTA LA REPUTACIÓN DE LOS BANCOS EN MATERIA DE SEGURIDAD A LA HORA DE ELEGIR A QUIÉN DEBEN CONFIAR SUS CUENTAS. [10]

EL 82 % AFIRMÓ QUE CONSIDERARÍA LA POSIBILIDAD DE DEJAR UN BANCO QUE HUBIERA SUFRIDO UNA FILTRACIÓN DE DATOS.[11]

Aunque los bancos ya disponen de cierto nivel de protección contra el fraude, ¿realmente es suficiente mantener un banco seguro y proteger las valiosas relaciones con los clientes?

Los servicios financieros online de todos los bancos están amenazados. Cientos de millones de dólares están en juego. Cualquier incidente de seguridad puede costar dinero y tiempo al banco, además de poner en peligro las relaciones a largo plazo con clientes fieles. Hoy en día, los sistemas de seguridad que fueron fiables en el pasado pueden hacer solo lo justo. Las personas siguen siendo el eslabón más débil en la cadena de seguridad, y se necesita protección proactiva para evitar que un simple error se convierta en una costosa crisis.

Kaspersky Fraud Prevention añade un nivel de defensa fundamental a la protección contra el fraude existente del banco. Protege a los clientes de los bancos que utilizan un PC o un Mac (a través de Kaspersky Fraud Prevention for Windows y Kaspersky Fraud Prevention for Mac), y Kaspersky Fraud Prevention Mobile SDK ayuda a proteger a los usuarios que prefieren acceder a sus cuentas bancarias a través de dispositivos móviles.

Kaspersky Fraud Prevention no solo soluciona los problemas después de un incidente de fraude: además, permite a los bancos tomar medidas proactivas para detener a los estafadores para que no puedan hacer más daño. Evita de forma activa que los cibercriminales puedan seguir robando los datos de los usuarios, ayudando así a eliminar las causas de fraude.

Además, nuestra inteligencia ayuda a asegurar que nuestros clientes bancarios permanecen protegidos, a pesar de la constante transformación del panorama de amenazas.

SOLO EL 51 % CREE QUE LAS ENTIDADES FINANCIERAS HACEN LO SUFICIENTE PARA PROTEGER LA INFORMACIÓN DELICADA.[12]

[10, 11 y 12] Informe de riesgos de IT globales de 2014, Kaspersky Lab

KASPERSKY LAB PROCESA AUTOMÁTICAMENTE MÁS DE 325 000 MUESTRAS DE MALWARE NUEVO CADA DÍA.

Y en un clima en el que los ciberataques son cada vez más y sofisticados y los criminales que los desencadenan innovan continuamente, no basta con limitarse a reaccionar cada vez que ocurre algo. A menos que los equipos de seguridad de IT de una empresa entiendan perfectamente la naturaleza de las amenazas a las que se enfrentan, defenderse contra ellas es imposible.

Al compartir nuestra inteligencia más reciente con nuestros clientes, ayudamos a las empresas a protegerse contra las amenazas. Nuestra amplia gama de servicios de inteligencia ayuda a garantizar que el centro de operaciones de seguridad (SOC, del inglés "security operations centre") o el equipo de seguridad de IT de una empresa está equipado para proteger a la empresa frente a las últimas amenazas online.

Incluso si su empresa no utiliza productos de Kaspersky Lab, puede beneficiarse de Security Intelligence Services.

Los servicios de inteligencia de seguridad de Kaspersky Lab supervisan constantemente el panorama de amenazas identificando peligros emergentes y adoptando medidas para combatirlos y erradicarlos. De este modo, sea cual sea la escala de la amenaza (desde correos electrónicos de phishing que suplantan a una marca hasta las tendencias globales de cibercrimen más recientes), nuestros clientes se benefician del acceso a la inteligencia de seguridad más reciente.

Además de la "inteligencia en bruto" y los informes personalizados, nuestros expertos también están disponibles para investigar los ataques lanzados contra un cliente específico. En estos casos, nuestros expertos identificarán a los autores, analizarán sus métodos y determinarán el mejor modo de anular la amenaza.

También ofrecemos servicios de formación que proporcionan a los SOC los conocimientos necesarios para detectar y responder a los ataques antes de que puedan causar daños.

La gama de servicios de inteligencia de seguridad que ofrecemos incluye los siguientes:

- Inteligencia frente a amenazas
  - Fuentes de datos de amenazas
  - Seguimiento de las amenazas de botnet
  - Creación de informes de inteligencia
- Servicios de formación
  - Principios básicos de la ciberseguridad
  - Ciencia forense digital
  - Análisis de malware e ingeniería inversa
- Servicios de investigación
  - Análisis de malware
  - Ciencia forense digital
  - Respuesta a incidentes

EL LIBRO DE REGISTROS DE CIBERATAQUES DIRIGIDOS <HTTPS://APT.SECURELIST.COM/> RECOPILA INNOVADORAS CIBERCAMPAÑAS MALICIOSAS INVESTIGADAS POR EL EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL (GREAT) DE KASPERSKY LAB.

KASPERSKY lab

EL PODER DE LA PROTECCIÓN

PROTECCIÓN LÍDER EN EL MUNDO CONTRA AMENAZAS CONOCIDAS, DESCONOCIDAS Y SOFISTICADAS.

Kaspersky Lab opera en más de 200 países y territorios de todo el mundo, y nuestras tecnologías protegen a más de 400 millones de personas y 270 000 empresas. Empleamos a más de 3000 especialistas altamente cualificados, liderados por nuestro director ejecutivo y presidente Eugene Kaspersky, que, entre sus múltiples reconocimientos internacionales, fue nombrado "pensador global" más destacado por la revista Foreign Policy en 2012.

Nuestro equipo de investigación y análisis global (GReAT) se compone de los mejores analistas del sector. Es una parte integral de nuestro departamento de I+D, y el equipo es líder en inteligencia, investigación e innovación contra amenazas, tanto a nivel interno como externo. Nuestros clientes se benefician asimismo de la red Kaspersky Security Network, que procesa en tiempo real datos relacionados con ciberseguridad para permitirnos ver con antelación las nuevas amenazas y permitirnos desarrollar tácticas defensivas.

Además de ayudar a empresas y particulares a protegerse contra las amenazas a la ciberseguridad, también cooperamos con respetados organismos internacionales y locales. Nuestro trabajo con Interpol y Europol, así como con organismos de las fuerzas del orden nacionales y regionales de todo el mundo, se centra en la implementación de tácticas defensivas destinadas a frustrar operaciones de malware y actividades cibercriminales.

Durante nuestras investigaciones, nuestros expertos técnicos analizan todos los elementos de un ataque, desde sus vectores de infección y componentes de malware, hasta su infraestructura de mando y control y los métodos de explotación que emplea. La información obtenida la vertemos en todas nuestras soluciones, lo que nos ayuda a detectar y rechazar los ataques de malware, independientemente de su origen y propósito.

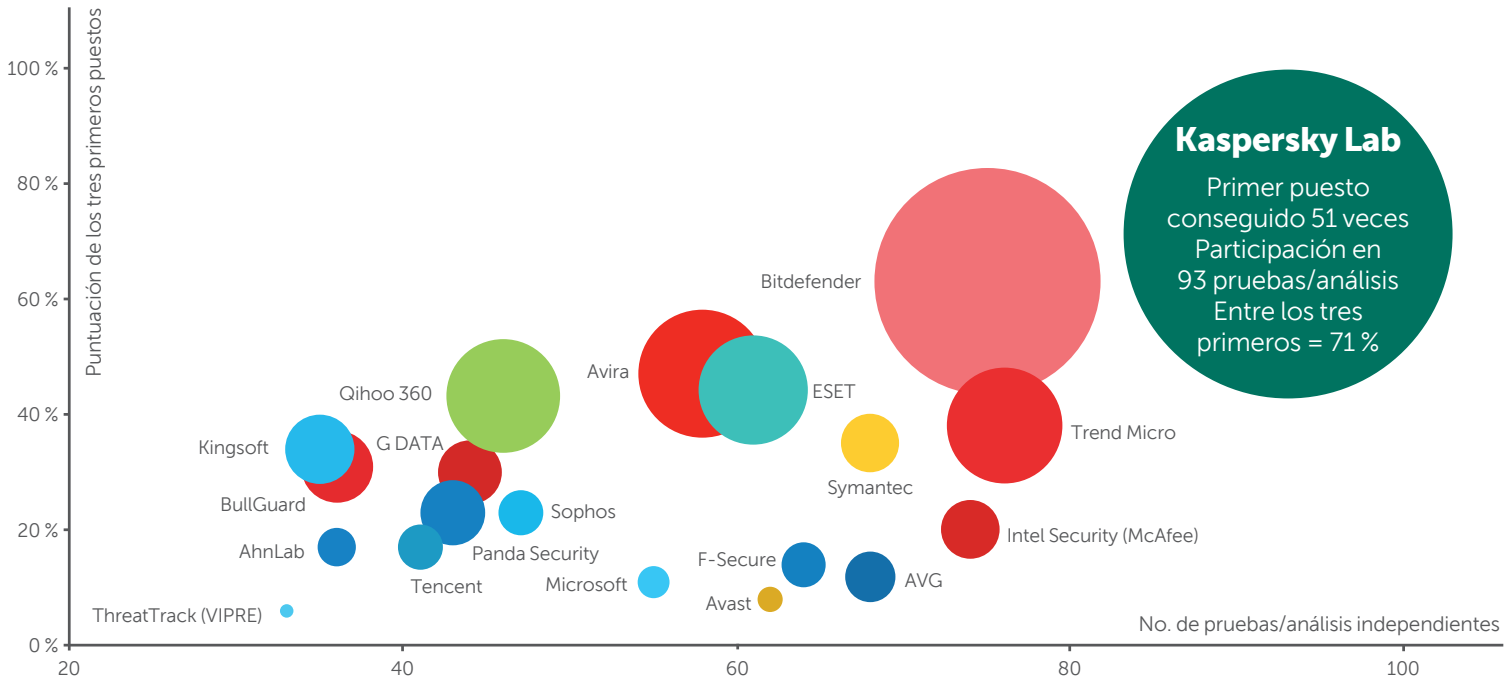
En estos momentos, estamos desarrollando un sistema operativo seguro y también estamos trabajando en soluciones que protejan contra los efectos potencialmente devastadores de los ataques a infraestructuras vitales.

No exageramos si decimos que nuestra misión consiste en salvar del cibercrimen al mundo:

- Los resultados de pruebas independientes demuestran consistentemente que Kaspersky Lab ofrece la mejor protección del sector. Solo en el año 2014, hemos participado en 93 pruebas y revisiones independientes. En 51 ocasiones, nuestros productos se colocaron en primer puesto, y en un 71 % de las pruebas Kaspersky Lab acabó entre los tres primeros.
- Más de un tercio de nuestro personal trabaja en I+D, proporcionando un crecimiento del 38 % en patentes de tecnología entre 2012 y 2013.
- Fuimos los primeros en descubrir muchas de las amenazas más sofisticadas del mundo, como Carbanak, Equation, DarkHotel, Regin, Duqu, Flame, Gauss, Octubre Rojo, Icefog y The Mask.
- Alrededor de 120 empresas líderes del sector confían en nosotros para ayudarlas a proteger a sus clientes, además de utilizar Kaspersky Lab para la integración tecnológica, el etiquetado privado o y los productos de marca compartida, la instalación previa y la venta en lotes de nuestros productos.

KASPERSKY LAB OFRECE LA MEJOR PROTECCIÓN DEL SECTOR*

DURANTE 2014, LOS PRODUCTOS DE KASPERSKY LAB PARTICIPARON EN 93 PRUEBAS Y REVISIONES INDEPENDIENTES. NUESTROS PRODUCTOS ACABARON EN 51 PRIMEROS PUESTOS Y 66 VECES ENTRE LOS TRES PRIMEROS.[13]



*Notas:
Según los resultados sintéticos de una prueba independiente realizada en 2014 para productos dirigidos a empresas, consumidores y dispositivos móviles.

El resumen incluye pruebas realizadas por los siguientes laboratorios y revistas independientes: Pruebas de laboratorio: AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin. El tamaño de la burbuja representa el número de primeros puestos obtenidos.

[13] http://media.kaspersky.com/en/business-security/TOP3_2014.pdf

PROTEGEMOS EL PRESENTE PARA ASEGURAR EL FUTURO

Un panorama de amenazas cada vez más sofisticado y complejo exige una plataforma de seguridad en varios niveles que proteja contra amenazas conocidas, desconocidas y sofisticadas.

Visite **kaspersky.com/enterprise** para obtener más información sobre la experiencia exclusiva de Kaspersky Lab y Security Solutions for Enterprise.

MÁS INFORMACIÓN

ÚNASE A LA CONVERSACIÓN

#EnterpriseSec

Véanos en YouTube

Síganos en Facebook

Síganos en Twitter

Únase a nosotros en LinkedIn

Revise nuestro blog

Únase a nosotros en Threatpost

Véanos en Securelist

ACERCA DE KASPERSKY LAB

Kaspersky Lab es el mayor proveedor privado de soluciones de protección de endpoints del mundo. La empresa figura entre los cuatro proveedores principales de soluciones de seguridad para usuarios de endpoints.* A lo largo de sus más de 17 años de historia, Kaspersky Lab se ha mantenido como una empresa innovadora en seguridad de IT y suministra eficaces soluciones de seguridad digitales para grandes empresas, pymes y particulares. Kaspersky Lab, cuya sociedad de cartera está registrada en el Reino Unido, opera actualmente en casi 200 países y territorios de todo el mundo, y brinda protección a más de 400 millones de usuarios en todo el mundo. Más información en www.kaspersky.es.

* La empresa logró el cuarto puesto en el índice de IDC de ingresos de seguridad para endpoints en todo el mundo por proveedor de 2013. Este índice se publicó en el informe de IDC "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (Previsión de seguridad mundial de endpoints 2014-2018 y acciones de los proveedores en 2013) (IDC núm. 250210, agosto de 2014). En el informe se clasifican los proveedores de software según los ingresos de ventas de soluciones de seguridad para endpoints en 2013.