KASPERSKY LAB: GARANTÍA DE CIBERSEGURIDAD INDUSTRIAL

KASPERSKY lab

Líder mundial reconocido en seguridad empresarial, Kaspersky Lab está desarrollando un papel de liderazgo a la hora de cubrir las necesidades exclusivas de la seguridad industrial.

LIDERAZGO DE KASPERSKY LAB

KASPERSKY LAB: GARANTÍA DE SEGURIDAD Y LIDERAZGO EN UNA VISIÓN DE FUTURO.

Kaspersky Lab, la empresa de ciberseguridad privada más grande del mundo, tiene más de 300 millones de usuarios repartidos entre 200 países y territorios de todo el mundo. Kaspersky Lab cuenta con una base de clientes corporativos de más de 250 000 empresas en todo el mundo, desde pymes hasta organizaciones comerciales y gubernamentales de gran tamaño. Más de 300 millones de personas en todo el mundo cuentan con la protección de los productos y las tecnologías de Kaspersky Lab.

Bajo la dirección de Eugene Kaspersky, su fundador y director ejecutivo, reconocido experto en ciberseguridad y visionario, la empresa ha conseguido una merecida reputación de conocimiento inigualable sobre las amenazas locales y globales, y ha descubierto muchas de las amenazas más importantes de los últimos años, incluidos Dark Hotel, Flame, Gauss, mini-flame, Octubre Rojo, NetTraveler y The Mask, así como los recientes ataques específicos industriales como Crouching Yeti (Energetic Bear), Miancha y Black Energy 2.

LIDERAZGO EN INTELIGENCIA SOBRE AMENAZAS

Mientras que Kaspersky Security Network, nuestra compleja infraestructura distribuida, se alimenta de la inteligencia en tiempo real generada por más de 60 millones de usuarios de Kaspersky voluntarios en todo el mundo, nuestro equipo de análisis e investigación global (GReAT, del inglés "Global Research and Analysis Team") de élite aporta un conjunto único de habilidades y experiencia a la investigación sobre amenazas de Kaspersky Lab, desarrollando soluciones capaces de combatir código de malware cada vez más complejo y sofisticado.

LIDERAZGO EN INVESTIGACIÓN E INNOVACIÓN

Como es una empresa privada, Kaspersky Lab tiene absoluta libertad para realizar importantes inversiones en investigación y desarrollo lejos de las restricciones del mercado a corto plazo. Casi la mitad de nuestros 3000 empleados a nivel mundial trabajan en nuestro laboratorios de investigación y desarrollo, y se centran en el desarrollo de tecnologías innovadoras, la investigación en ciberguerras, ciberespionaje y cibersabotaje, y todos los tipos de amenazas y técnicas.

Este enfoque en I+D interno de alta calidad ha llevado a que Kaspersky Lab se reconozca como un líder en el sector en lo que se refiere a tecnologías de ciberseguridad, y pruebas independientes siguen ofreciendo más puntuaciones excepcionales a Kaspersky Lab que a ningún otro proveedor.

PARTNER DE CONFIANZA DE GOBIERNOS Y ORGANISMOS REGULADORES

La investigación sobre amenazas siempre ha sido una parte integral de la estrategia de Kaspersky Lab. Con reconocidos investigadores y analistas líderes en el sector de todo el mundo, la comunidad de ciberseguridad global y respetadas empresas internacionales, incluidas Interpol, Europol, Unidad de cibercrimen de Microsoft, agencias de ciberseguridad y numerosos CERTS, ISA (Sociedad Internacional de Automatización, del inglés "International Society of Automatization") han invitado a Kaspersky Lab a mantener la colaboración y el asesoramiento con ellos de forma regular. Actualmente trabajamos en estrecha colaboración con los organismos reguladores de Rusia y Estados Unidos, entre otros, para desarrollar marcos de seguridad industrial y protección de infraestructuras vitales.

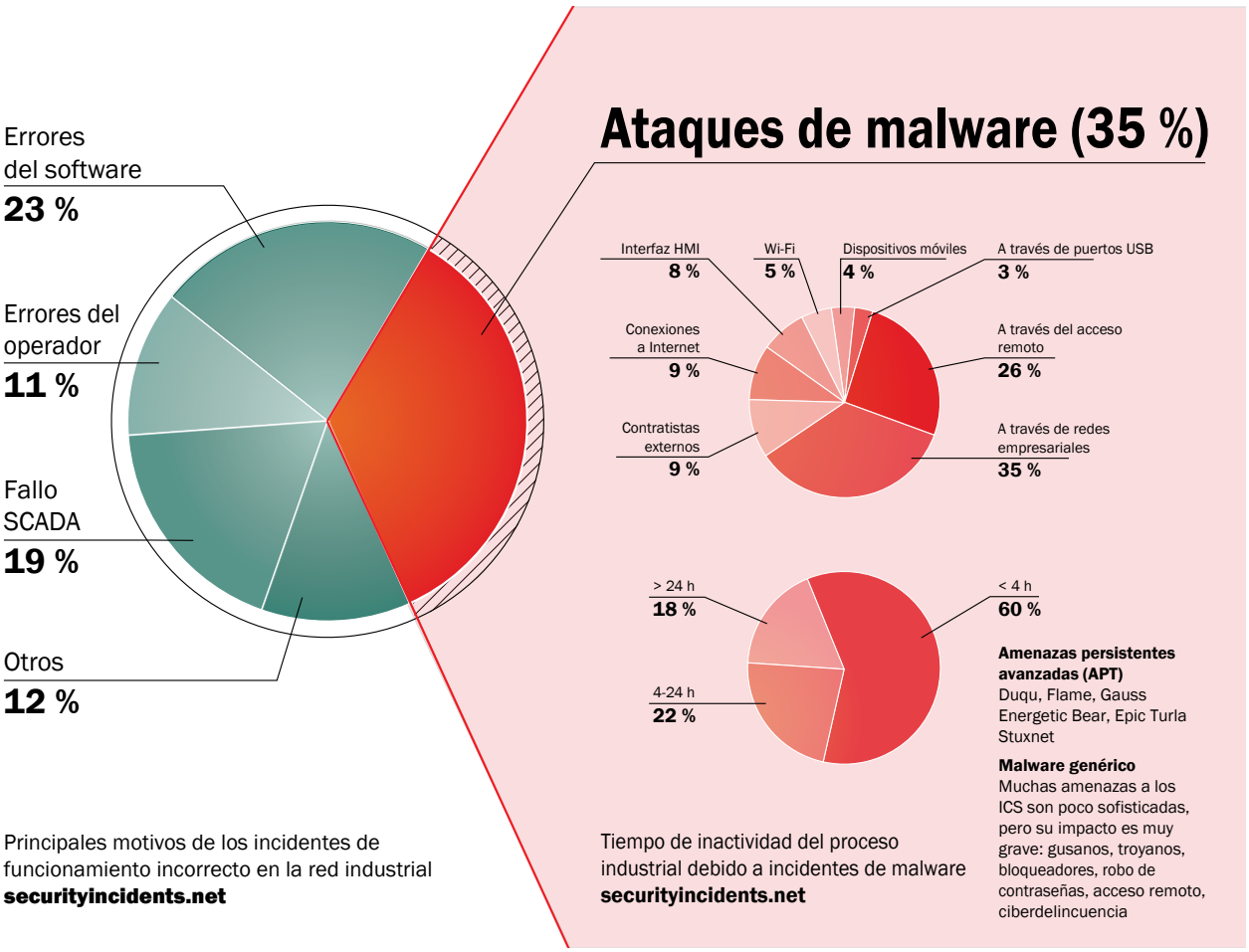
VISIÓN DE KASPERSKY LAB SOBRE EL ESTADO DE LA SEGURIDAD INDUSTRIAL

AMENAZAS: NO TIENE QUE SER UN OBJETIVO PARA CONVERTIRSE EN UNA VÍCTIMA; MOTIVOS POR LOS QUE LOS ENFOQUES DE SEGURIDAD INDUSTRIAL ACTUALES NO FUNCIONAN

Las recientes investigaciones llevadas a cabo por SANS Institute han detectado que solo el 9 % de los profesionales de IT del sector industrial dijeron que estaban seguros de que no habían sufrido filtraciones[1]. Sorprendentemente, el 16 % dijo que no había implementado ningún proceso para detectar vulnerabilidades, en parte por miedo a atraer la atención no deseada hacia las vulnerabilidades del sistema.

Pero no tiene que ser un objetivo para convertirse en una víctima. Además de amenazas persistentes avanzadas industriales específicas como Citadel, Crouching Yeti/Havex, Miancha o Black Energy 2, muchas de las amenazas y vulnerabilidades a las que se enfrentan los sistemas industriales hoy día provienen de amenazas diarias en el nivel empresarial de su infraestructura.

AMENAZAS: NO TIENE QUE SER UN OBJETIVO PARA CONVERTIRSE EN UNA VÍCTIMA



Principales motivos de los incidentes de funcionamiento incorrecto en la red industrial
securityincidents.net

Tiempo de inactividad del proceso industrial debido a incidentes de malware
securityincidents.net

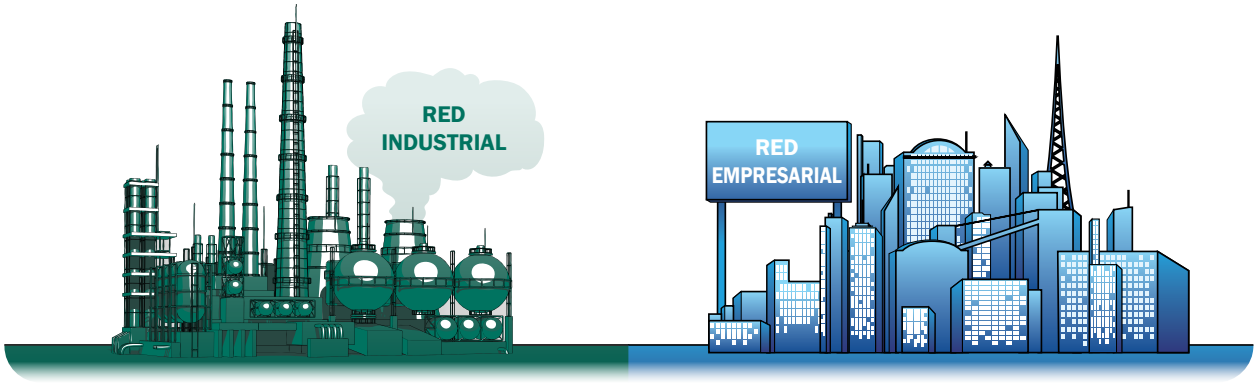
1 SANS Institute: 2014 Control System Security Survey (SANS Institute: encuesta de seguridad de sistemas de control de 2014)

Los ataques industriales específicos utilizan tanto la LAN de la empresa como los sistemas de control industrial (ICS) para atacar y propagarse; Energetic Bear infectó el servidor OPC y el software del equipo de los ICS con un troyano de acceso remoto, pero también aprovechó vulnerabilidades conocidas del software Adobe PDF para lanzar ataques de spear phishing. Los ataques se propagaron de un sistema a otro, robando información de sistemas SCADA y dañando ICS no reforzados borrando PC o sobrecargando redes.

El gusano Conficker, aunque no es específicamente industrial, no solo se ha encontrado en equipos médicos críticos, sino que se sospecha que ha sido una "puerta abierta" para ataques industriales de alto perfil como Stuxnet. Conficker es capaz de sobrecargar completamente las redes y detener totalmente los procesos vitales. Las técnicas de seguridad industrial tradicionales no abordan estas amenazas demasiado bien: la estrategias de "brecha de aire" o "seguridad por anonimato" no abordan la realidad, que consiste en que los sistemas de red eléctrica inteligente y las aplicaciones basadas en web se traducen en que los "sistemas de control industrial cada vez se parecen más a los PC comerciales[2]."

LA SEGURIDAD INDUSTRIAL ES DIFERENTE

Hay una coincidencia general entre las amenazas, pero las diferencias entre los requisitos de la ciberseguridad industrial y los de las empresas generales son importantes. Muchas estrategias de seguridad de IT se centran en la protección de datos y confían en el concepto de C-I-D: confidencialidad, integridad y disponibilidad de los datos. Los sistemas industriales priorizan la continuidad por encima de todo; su protección no es para la **disponibilidad**, **integridad** y **confidencialidad** de los "datos", sino de los "procesos", en ese orden. Esto es lo que distingue las necesidades de seguridad industrial; incluso la solución de seguridad de más alta calidad es de hecho inútil si la continuidad del proceso es la que está riesgo. No se puede permitir que las técnicas de seguridad cotidianas como la protección antimalware, la gestión de parches, las actualizaciones de software y la gestión de la configuración de la seguridad repercutan de forma negativa en los procesos.



1. DISPONIBILIDAD
2. INTEGRIDAD
3. CONFIDENCIALIDAD

1. CONFIDENCIALIDAD
2. INTEGRIDAD
3. DISPONIBILIDAD

2 Agencia Europea de Seguridad de las Redes y de la Información (ENISA): "Can we learn from SCADA security incidents?" ("¿Podemos aprender de los incidentes de seguridad de SCADA?").

EL ENFOQUE CORRECTO PARA LA SEGURIDAD INDUSTRIAL

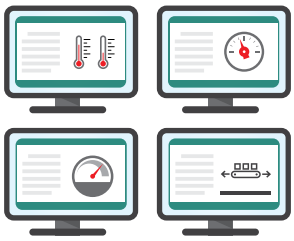
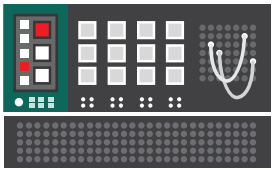
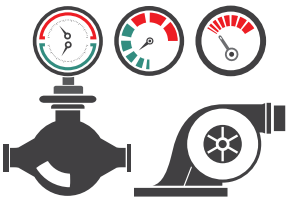
Estas necesidades diferentes de la seguridad industrial hacen que trabajar con el proveedor correcto sea extremadamente importante. Las soluciones de ciberseguridad industrial deberían incluir tres pilares fundamentales: un enfoque basado en los procesos para la implementación de la seguridad, la concienciación y formación de los empleados, y soluciones creadas específicamente para su uso en entornos industriales.

El enfoque de Kaspersky Lab para la seguridad industrial es un planteamiento amplio que incluye:

- La actitud correcta para abordar la seguridad industrial: no hay una fórmula milagrosa ni una solución inmediata. La implementación de la seguridad industrial es un proceso que comienza con una auditoría y otros servicios antes de pasar a la preparación de las personas para el cambio ni antes de iniciar la implantación gradual de soluciones especializadas y sin interferencias. Esta es la única manera de conseguir una protección perfecta y totalmente funcional. Porque cada minuto de tiempo de inactividad en el proceso de fabricación se traduce en costes importantes, la instalación de cualquier producto debe llevarse a cabo con la ayuda de expertos profesionales, disponibles de forma ininterrumpida.
- Las personas desempeñan un papel fundamental en cualquier estrategia de seguridad. La capacitación de los diferentes accionistas y equipos a través de formación, desde los ejecutivos de nivel C hasta los administradores de IT y los ingenieros de OT. Nuestro juego de rol Kaspersky Industrial Protection Simulation (KIPS), por ejemplo, permite que incluso el personal no técnico pueda comprender la importancia de la ciberseguridad y las necesidades de su lugar de trabajo.
- A nivel de tecnología, Kaspersky Lab ofrece soluciones basadas en tecnologías únicas, creadas específicamente para redes industriales: extremadamente tolerantes a fallos, sin interferencias en los procesos tecnológicos y capaces de trabajar en escenarios en los que se producen brechas en tiempo real.

▶ SOLUCIÓN DE KASPERSKY LAB

PROPUESTA DE VALOR DE KASPERSKY LAB

NIVEL 4 Planificación comercial y logística		Gestión integral de la cadena de suministro. Establecimiento del programa básico de la fábrica: producción, uso de materiales, distribución y envío.	Kaspersky Security for Business + Professional Services
NIVEL 3 Gestión de operaciones de fabricación		Control del flujo de trabajo/recepción para producir el producto final deseado. Mantenimiento de registros y optimización del proceso de producción.	
NIVEL 2, 1 Control por lotes. Control continuo. Control discreto.		Supervisión, control de supervisión y control automatizado del proceso de producción.	Kaspersky Industrial Security + Professional Services
		Detección del proceso de producción, manipulación del proceso de producción.	
NIVEL 0 Físico		Dispositivos físicos	Seguridad física

▶ VENTAJAS PARA EL CLIENTE

PROTECCIÓN TRIPLE

La solución de seguridad industrial de Kaspersky Lab cubre todos los aspectos de la ciberseguridad para los clientes industriales, como los proveedores de energía:

- En todos los niveles, desde la red a nivel empresarial hasta la planta de producción.
- Formación y concienciación para los ejecutivos de nivel C, IT, seguridad de IT e ingenieros.
- Garantía de la continuidad del negocio a través de la protección de datos y el proceso tecnológico.

OPCIONES DE SEGURIDAD INDUSTRIAL ESPECIALIZADAS Y ADAPTADAS

Kaspersky Lab entiende que cada red tecnológica tiene sus características específicas que, en la mayoría de los casos, son únicas. Nuestra solución industrial es completamente personalizable y funciona como un "conjunto de herramientas construcción" que se puede adaptar a las necesidades específicas de cada cliente y ajustarse a los retos, las demandas y las infraestructuras específicas únicas.

Al trabajar con Kaspersky Lab, los clientes industriales tienen acceso completo a más de una década de inteligencia y experiencia sobre ciberseguridad; nuestros consultores e ingenieros son un componente central de nuestro equipo de servicios profesionales. Porque cada minuto de tiempo de inactividad en el proceso de fabricación se traduce en costes importantes, la instalación de cualquier producto debe llevarse a cabo con la ayuda de expertos profesionales, disponibles de forma ininterrumpida. Además de los acuerdos de soporte y mantenimiento, también están disponibles los expertos de Kaspersky Lab para llevar a cabo investigaciones a fondo de los incidentes de seguridad, así como para entregar informes de inteligencia sobre las amenazas existentes, incluida la inteligencia sobre amenazas de nuestro equipo de expertos GReAT. Kaspersky Lab considera que la seguridad industrial más eficaz se consigue a través de una combinación de tecnología y servicios integrados de expertos. Entre los servicios expertos que Kaspersky Lab ofrece a los proveedores industriales se encuentran los siguientes:

- Auditoría, informes y recomendaciones sobre ciberseguridad, seguidos del desarrollo y la implementación de políticas y procedimientos, así como el soporte técnico necesario.
- Desarrollo de un modelo contra amenazas y recomendaciones de mitigación
- Respuesta ante amenazas: investigación de incidentes, ciencia forense digital (y análisis de malware) y asesoramiento jurídico.
- Formación específica sobre ICS y general sobre ciberseguridad
- Asesoramiento a organismos del estado y organismos reguladores industriales.

KASPERSKY LAB: EL FUTURO DE LA SEGURIDAD INDUSTRIAL

Gracias a nuestra experiencia en tecnologías de seguridad industrial a medida, Kaspersky Lab está desarrollando soluciones personalizables de forma activa para proteger las redes tecnológicas. Nuestra estrategia a largo plazo implica el desarrollo de un sistema operativo seguro, poniendo de manifiesto nuestra visión de ofrecer lo último en seguridad integrada básica para una amplia variedad de dispositivos similares a los PLC que se usan en las infraestructuras vitales, incluidas las industriales.

Kaspersky Lab ya es un proveedor de seguridad fiable y partner de empresas industriales líderes en el sector que han utilizado nuestra protección antivirus durante muchos años. Kaspersky Lab también colabora con los principales proveedores de automatización industrial, incluidos Emerson, Rockwell Automation, Siemens y otros, para establecer procedimientos especializados y marcos de cooperación en ciberseguridad con el fin de proteger los entornos industriales de las ciberamenazas existentes y emergentes (incluidas las APT), y garantizar la compatibilidad de las soluciones de Kaspersky Lab con la tecnología operacional del cliente. Esto demuestra nuestra capacidad de ofrecer seguridad industrial eficaz sin que ello repercuta en la continuidad y consistencia operacionales.

KASPERSKY LAB: EXPERTOS EN SEGURIDAD INDUSTRIAL ESPECIALIZADA

Según Forrester Research, las amenazas a la infraestructura vital e industrial no se pueden seguir ignorando, y aquellos encargados de la selección de los proveedores de seguridad deben "buscar la experiencia especializada en el sector".[3] El informe de Forrester identifica a Kaspersky Lab como uno de los pocos proveedores que ofrece soluciones de seguridad industrial especializadas que realmente cumplen sus promesas y tiene una verdadera experiencia y conocimientos en el sector.

Como líder reconocido en ciberseguridad y protección industrial, Kaspersky Lab investiga y desarrolla continuamente soluciones que trabajen más para abordar las amenazas en constante evolución a las infraestructuras industriales y vitales. Desde la gestión de las operaciones hasta el nivel SCADA y más allá, hasta un futuro donde los entornos operativos seguros sean una realidad, Kaspersky Lab está jugando un papel protagonista para ayudar al sector, los organismos reguladores y las agencias gubernamentales a nivel global a anticiparse a los cambios en el panorama de amenazas y defenderse contra los ataques.

La seguridad industrial tiene consecuencias que van mucho más allá de la protección de las empresas y la reputación. En muchos casos, existen muchas consideraciones ecológicas, sociales y macroeconómicas importantes a tener en cuenta a la hora de proteger los sistemas industriales de las ciberamenazas. A medida que aumentan las amenazas dirigidas a infraestructuras industriales vitales, elegir el mejor consejero y partner tecnológico para asegurar sus sistemas nunca había sido tan importante. ¿Por qué no llama a los expertos de Kaspersky Lab para obtener más información sobre el futuro de la ciberseguridad industrial?

3 Forrester Research, *S&R Pros Can No Longer Ignore Threats to Critical Infrastructure* (Los profesionales de seguridad y riesgo no pueden seguir ignorando las amenazas a la infraestructura vital), por Rick Holland.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab
www.kaspersky.es

Todo sobre la seguridad
en Internet:
www.viruslist.com/sp

Encuentre un partner próximo:
http://www.kaspersky.es/partners/
socios-kaspersky

KASPERSKY lab