G DATA | SIMPLY SECURE

INGENIERÍA SOCIAL Y ERRORES DE CAPA 8…

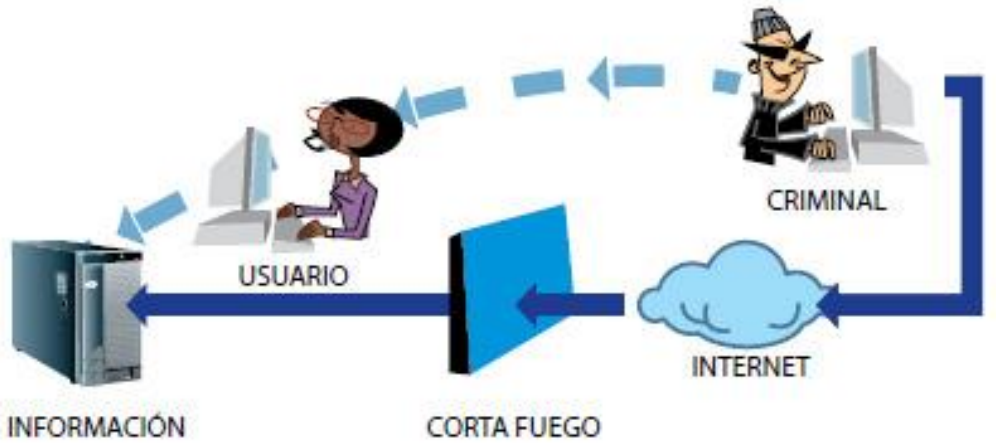
¿Que tan preparados estamos para enfrentar las nuevas infecciones y sus consecuencias?

SOFTHARD
Intelligent Safety

SE DICE A MENUDO QUE LA UNICA COMPUTADORA SEGURA ES AQUELLA, QUE NUNCA SERA ENCENDIDA.

¿QUÉ ES LA INGENIERÍA SOCIAL?

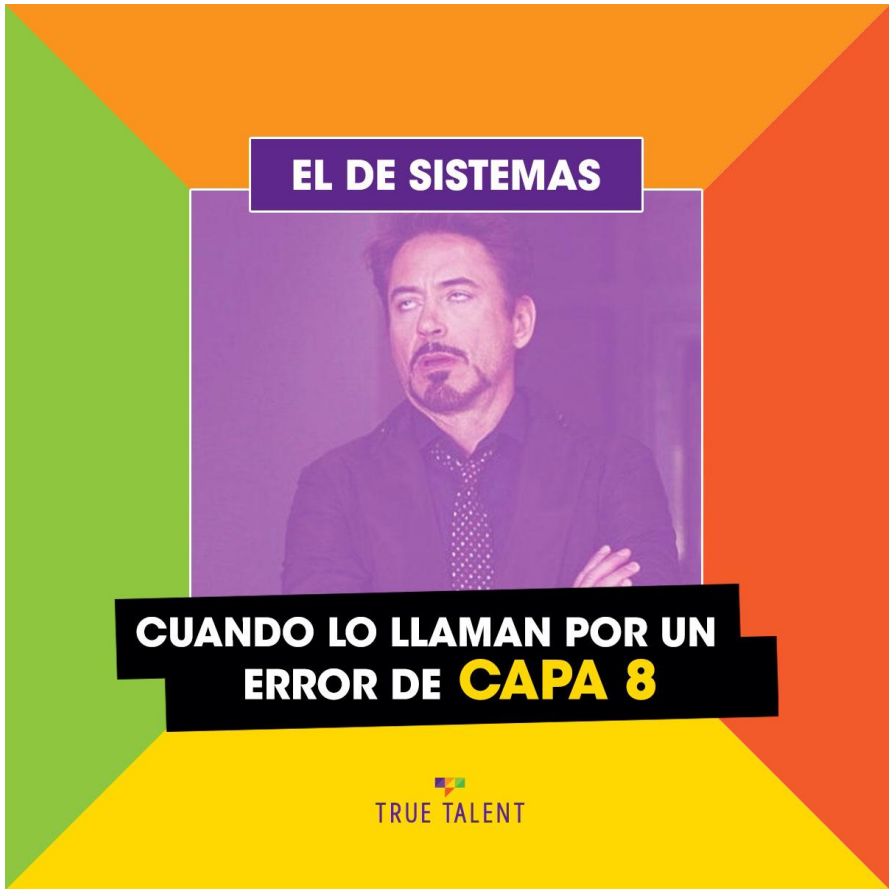
- La ingeniería social comprende diversos trucos psicológicos que tienen lugar en el marco del espionaje económico para arrebatar a los trabajadores datos relacionados con la seguridad. Los responsables de los ataques hacen acopio de dicha información y no solo se infiltran en los sistemas informáticos, sino que a través de ellos también consiguen acceder a los datos protegidos de las empresas. Se pone en práctica, así, el llamado social hacking. Además, la ingeniería social también entra en juego para llevar a los empleados de las empresas a reacciones poco meditadas o imprudentes, entre las que se engloban la instalación de programas desconocidos o la realización de transacciones financieras sospechosas.

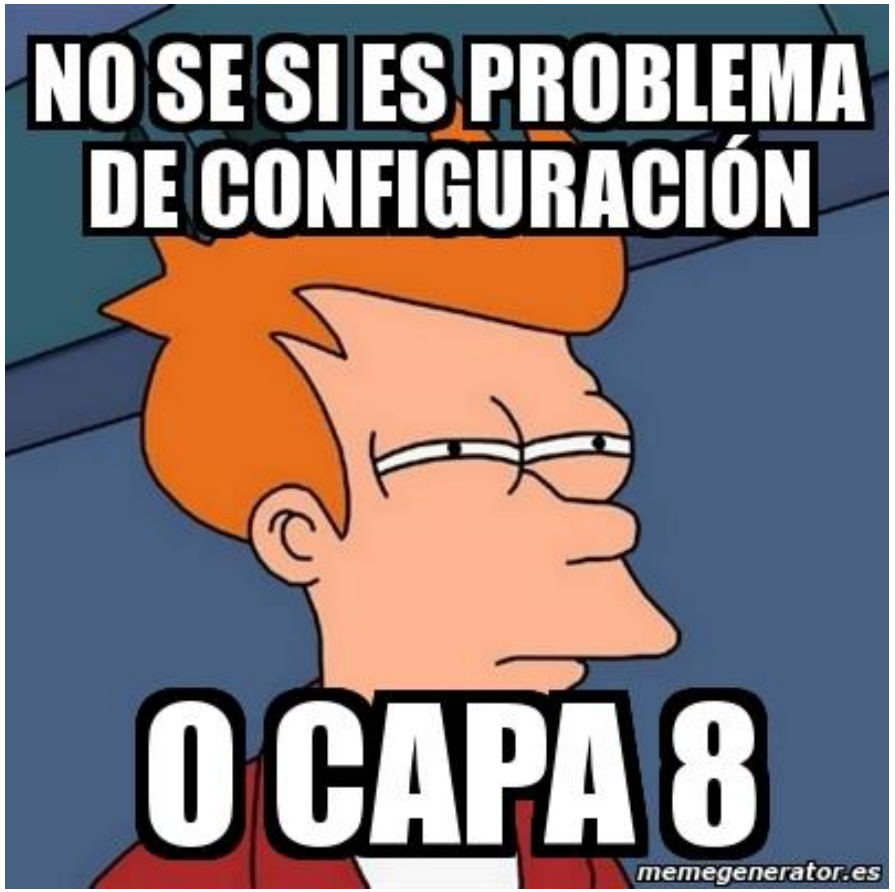


SOFTHARD
Intelligent Safety

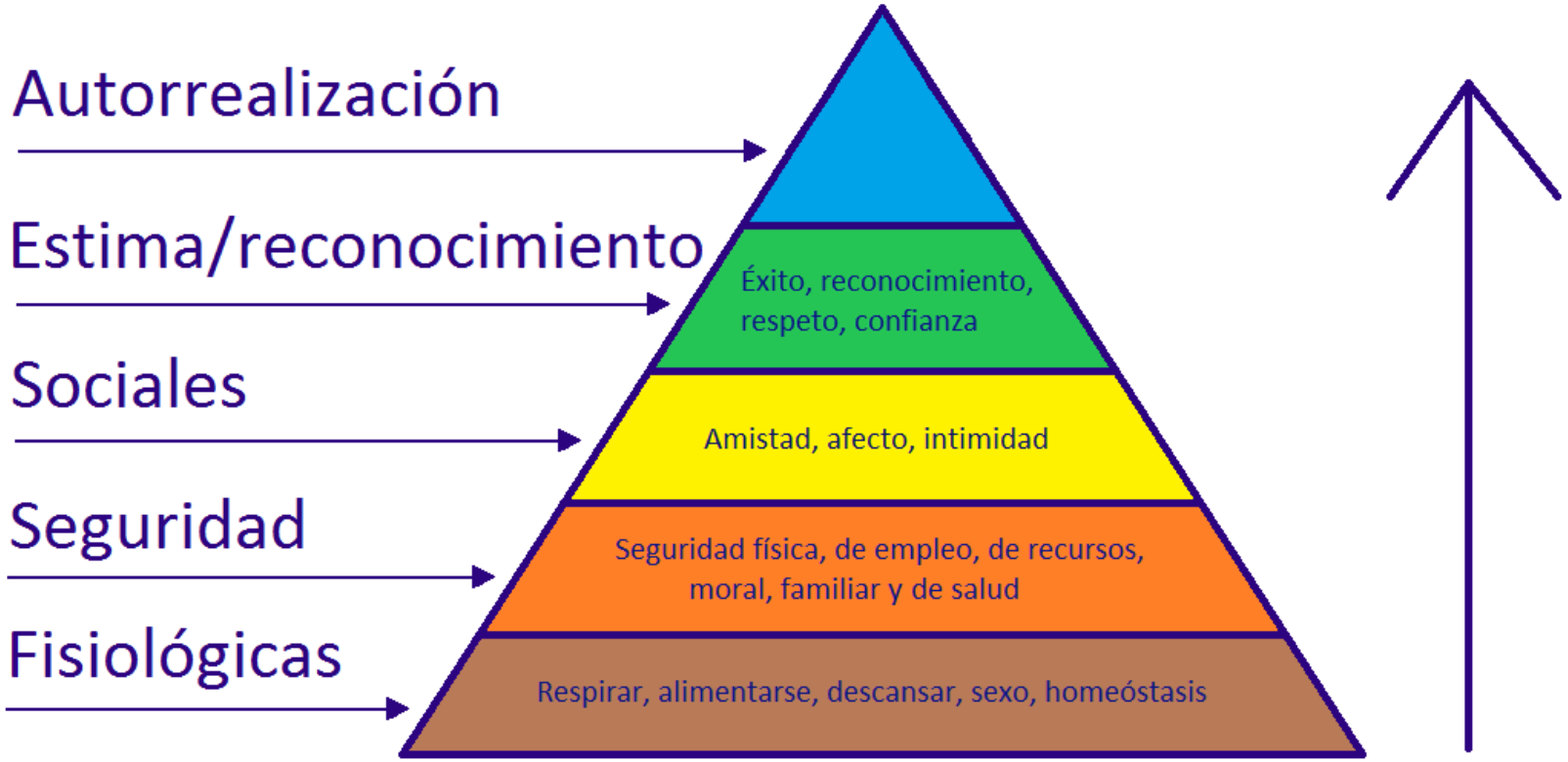
QUE ENTENDEMOS POR CAPA FICTICIA…

- Los especialistas en informática se esfuerzan por lograr que haya seguridad en todas las capas del modelo OSI. A menudo, las pérdidas no se ocasionan en la propia red, sino que tienen lugar en la capa 8 ficticia, es decir, a cuarenta centímetros de la pantalla, donde los usuarios interactúan con la técnica. Los **estafadores** lo saben, por lo que se aprovechan de cualidades y conductas humanas típicas, tales como la buena disposición, la confianza, el respeto, el orgullo, la gratitud, la prevención de conflictos o el miedo, para acceder a los sistemas informáticos sin autorización. Se puede hablar en este caso del método del social engineering, que cada año y a nivel mundial ocasiona daños valorados en miles de millones, por lo que para las empresas resulta imprescindible formar a sus trabajadores y darles directrices claras sobre el **tratamiento adecuado de la información confidencial**.


EL DE SISTEMAS
CUANDO LO LLAMAN POR UN ERROR DE CAPA 8
TRUE TALENT


NO SE SI ES PROBLEMA DE CONFIGURACIÓN
O CAPA 8
memegenerator.es

PIRÁMIDE DE MASLOW



LOS TRES MOTORES DE UN ATAQUE

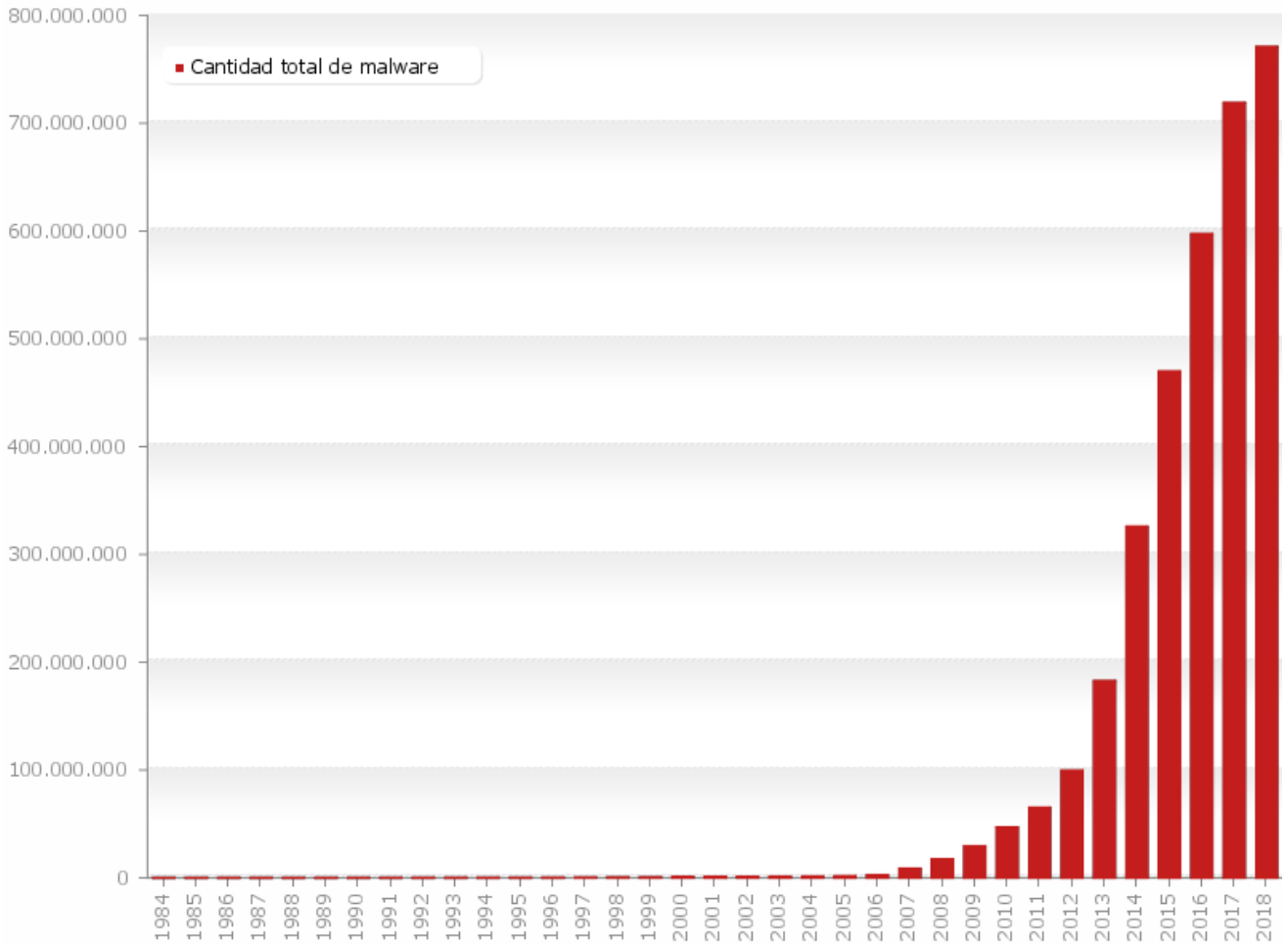
- Motivo: En primer lugar, los propietarios de activos informáticos deben concientizarse en que los mismos, por más privados y ocultos que se encuentren, son una tentación para personas u organizaciones tanto internas como externas a su uso. En este sentido, se pueden identificar diversos motivos como son: autoconocimiento, dinero, venganza, competencia e información entre otros.
- Oportunidad: En segundo lugar, mientras no existan mecanismos(administrativos y tecnológicos) formales de protección a activos informáticos, los mismos se encuentran vulnerables y presentan un alto riesgo de recibir un ataque.
- Conocimiento: Finalmente, se debe de entender que probablemente se tengan las políticas de seguridad más rigoristas y la tecnología de seguridad más avanzada, sin embargo siempre existirá un posible atacante lo bastante preparado como para vulnerar los activos informáticos

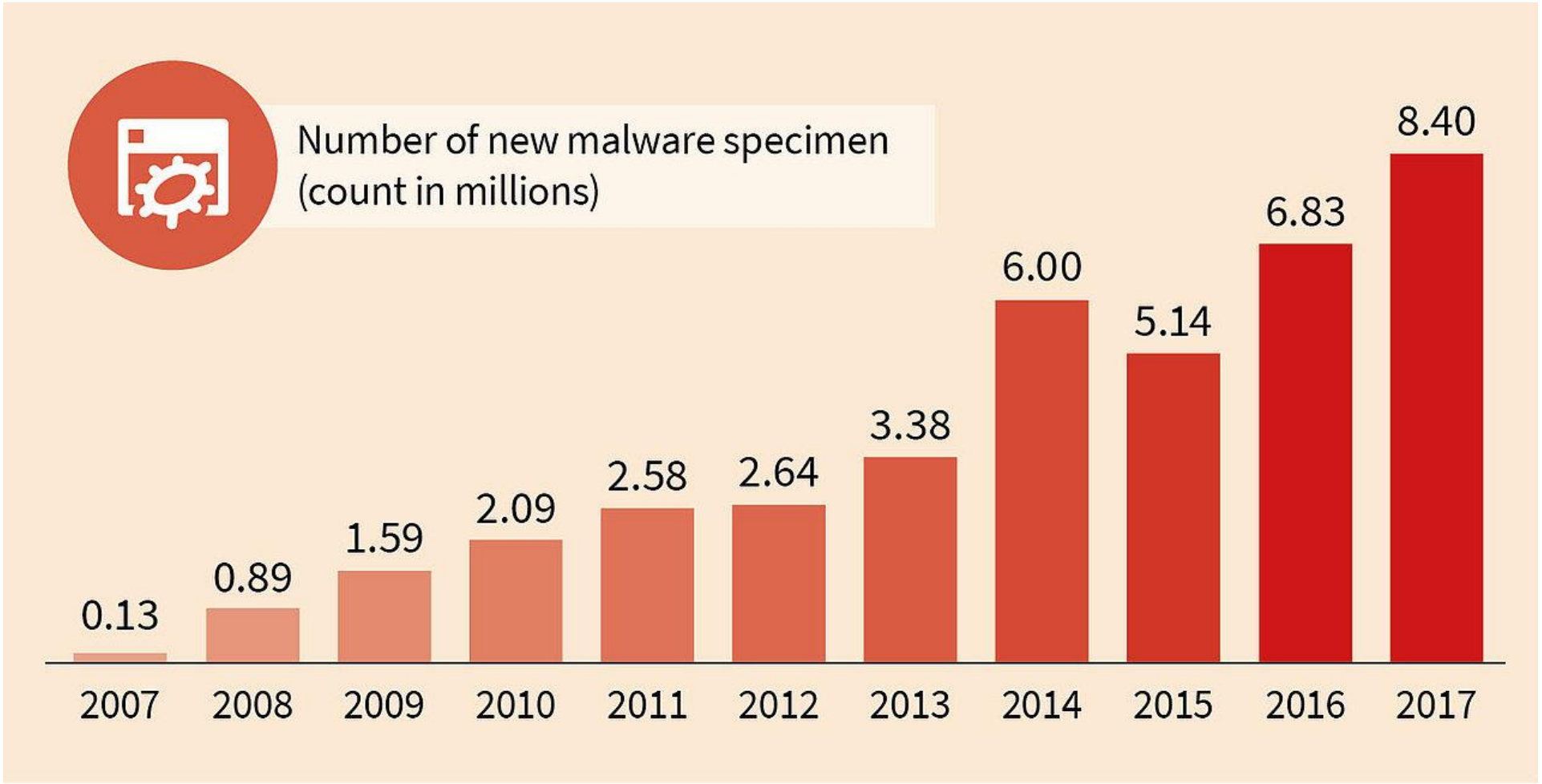
¿CUÁLES SON SUS CONSECUENCIAS?

- Actualmente, la globalización ha permitido descubrir que no sólo esta expuesta al terrorismo cibernético la infraestructura básica de servicios públicos de un país, sino que ahora sus objetivos son además, sitios de la red, servidores de comercio, correos electrónicos, y hasta la misma infraestructura operativa y comercial crítica de una empresa en su conjunto. La lista de objetivos potenciales incluye empresas industriales, comerciales y de servicios, centrales eléctricas, bancos y seguros, aerolíneas, sistemas de control de tráfico aéreo, transporte y logística, instalaciones petroleras y gasíferas, químicas y petroquímicas, procesadoras de alimentos, centros de salud y entidades gubernamentales, etc

ORIGEN DE LOS SPAM SEGÚN PAIS.

CANTIDAD TOTAL DE MALWARE




Number of new malware specimen
(count in millions)
0.13
0.89
1.59
2.09
2.58
2.64
3.38
6.00
5.14
6.83
8.40
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

G DATA ENDPOINT PROTECTION BUSINESS

- Nuestro software antivirus cierra los agujeros de seguridad que aprovechan todos los cibercriminales: nuestras medidas de seguridad proactivas y reactivas se complementan perfectamente para contrarrestar ciber amenazas de cualquier tipo: virus, gusanos, troyanos... Las soluciones empresariales de **G DATA** incorporan además muchas otras funcionalidades para facilitar la administración de todos los componentes de la red, protegiendo al mismo tiempo los datos confidenciales de su empresa. Consiga una visión general de los parches que afectan a la seguridad así como de las aplicaciones de su red desde una única consola de gestión.

SOFTHARD
Intelligent Safety

¿QUÉ ES POSIBLE CON G DATA?

59 % El 59 % de las empresas han sido víctimas de algún ciberataque en los últimos dos años.

54 % El 54 % de las empresas afectadas por ciberataques que consiguieron su objetivo aluden a un descuido de sus empleados como causa principal.

36 % El 36 % atribuyen el éxito de los ataques a parches no instalados.

Fuente: BSI (Oficina Federal para la Seguridad en las Tecnologías de la Información) 2015

- Los ciberdelincuentes no se infiltran en las redes empresariales exclusivamente a través de Internet. Uno de cada dos ciberataques tiene su origen en empleados que introducen el software malicioso en el sistema, ya sea de forma consciente o totalmente involuntaria. Basta una memoria USB convenientemente manipulada en manos de un empleado curioso que quiera saber qué secretos guarda. Almacenar información sensible en soportes externos es otra forma de dañar a una compañía. Y, actualmente, a los empleados de cualquier organización les resulta muy sencillo llevarse la información confidencial de su empresa en cualquier tipo de memoria externa. Las medidas de control por clientes consiguen reducir al mínimo los riesgos asociados a los procesos internos de la propia empresa y garantizan la integridad de los datos, además de mejorar la productividad de la propia compañía.

SOFTHARD Intelligent Safety

NUESTRAS SOLUCIONES

- **Control de dispositivos:** Limite el uso de dispositivos externos como grabadoras o memorias USB e impida que los datos de su empresa caigan en manos indebidas.

- **Control de aplicaciones:** Minimice riesgos y elija usted mismo qué programas pueden instalar los empleados en sus equipos.

- **Control de contenido web:** Defina en una lista blanca o negra qué páginas web se pueden visitar o no desde cualquiera de los clientes de su red empresaria.

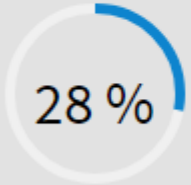
- **Patch Management:** Este módulo detecta automáticamente los agujeros de seguridad no parcheados en todos los programas instalados en su red. Así podrán cerrarse rápidamente todas las vulnerabilidades de, por ejemplo, el sistema operativo Windows, en uno en todos los clientes de la red empresarial.

SOFTHARD
Intelligent Safety

Mobile Device Management

8400

G DATA detecta una media de 8.400 nuevas amenazas para Android cada día.



El 28 % de las empresas afectadas por acciones de espionaje, sabotaje y robo de datos aluden al robo de dispositivos móviles como el origen más probable de los ataques.

Fuente: G DATA/Bitkom, Spionage, Sabotage and Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter, Studienbericht 2015

- Con la estrategia de gestión correcta, puede poner fácilmente en práctica el concepto «bring your own device»: con G DATA Administrator también puede gestionar los dispositivos móviles de su red de acuerdo a sus necesidades. De esta forma, los smartphones y tabletas con Android o iOS pueden integrarse en la infraestructura TI de su empresa y protegerse sin problemas. La combinación de controles de acceso y gestión de dispositivos hace posible un acceso remoto seguro y controlado a los servicios y recursos: los empleados que no se encuentran en las instalaciones de la empresa pueden acceder también a su correo electrónico, calendario y notificaciones.

SOFTHARD
Intelligent Safety

NUESTRAS SOLUCIONES

- **Protección en tiempo real:** La protección web protege todas las actividades en el navegador de los dispositivos Android. Se comprueban las apps descargadas en tiempo real para detectar componentes dañinos, pero también es posible realizar análisis bajo demanda de todo el dispositivo.

- **Protección antirrobo:** Localice fácilmente su dispositivo Android en caso pérdida o robo, bloquéelo o, en caso necesario, borre todos los contenidos de forma remota.

- **Filtro de apps:** Limite en su red el uso de apps y contenidos multimedia en los dispositivos móviles.

- **Filtro de contactos:** Gestione los contactos en los dispositivos Android utilizando la agenda corporativa. Cree así filtros específicos de llamadas y SMS.

SOFTHARD
Intelligent Safety

ALGUNOS CUIDADOS ADICIONALES…

- **Desconfianza saludable frente a personas ajenas a las empresa:** cuanto más grande es una empresa, más fácil es que las personas ajenas a ella se hagan pasar por trabajadores o por prestadores de servicios. Ante el peligro de desvelar datos internos de la empresa involuntariamente, lo conveniente es optar por el papel protector que generalmente plantea tener una desconfianza saludable frente a personas ajenas. Solo se deberían transmitir datos confidenciales a aquellos compañeros de trabajo cuya identidad pueda garantizarse sin ninguna duda.
- **Información proporcionada por teléfono:** es fundamental que nunca se faciliten datos confidenciales por teléfono, lo que se debe aplicar, sobre todo, a llamadas entrantes y de interlocutores desconocidos. Además, la información que aparentemente es secundaria sirve de ayuda a los timadores para recopilar información sobre las empresas y para, en la medida de lo posible, engañar a otros compañeros.
- **Correos electrónicos con remitente desconocido:** si no es posible identificar al remitente de un correo electrónico con total seguridad, se recomienda ser cauteloso. Los trabajadores deberían consultar en todo caso a un superior o a una persona del departamento de informática antes de responder a ese tipo de mensajes. Si el mensaje requiere llevar a cabo una acción inesperada, como por ejemplo una transferencia algo sospechosa, es conveniente realizar una llamada de contestación al supuesto remitente.

- **Atención con archivos adjuntos en enlaces y correos electrónicos:** los usuarios de Internet siempre encuentran en sus bandejas de entrada correos electrónicos con enlaces a máscaras para introducir datos. Los timadores utilizan técnicas de esta índole para acceder a bases de datos, contraseñas o números de cliente, de modo que en el mundo empresarial estas prácticas no son nada inusuales. En principio, los bancos, tiendas online o compañías de seguros serios no piden a sus clientes que para crear una página web tengan que facilitar datos sensibles, pero se insta a ser especialmente cuidadoso en el caso de los archivos adjuntos, ya que estos pueden contener malware que se instale en un segundo plano y que permita acceder al sistema. Lo recomendable en este caso es minimizar el riesgo de que se incite a los trabajadores a abrir los archivos adjuntos de correos electrónicos procedentes de remitentes desconocidos.
- **Protección de datos en las redes sociales:** la preparación de los ataques de ingeniería social tiene lugar, por lo general, mucho antes de que se produzcan los ataques en sí. Además de las páginas web de las empresas, las redes sociales son también una gran fuente de información para los estafadores, cuyo objetivo es disfrazar los intentos de manipulación y darles un carácter creíble. En general, cuanta más información revele un trabajador sobre sí mismo en la red, mayor es el riesgo de verse afectado por la técnica del social engineering. De ello se desprende que es muy importante informar a los trabajadores sobre las configuraciones de privacidad y ofrecerles normas claras para manejar los contenidos corporativos en las redes sociales.

·Crear la CULTURA de la cautela, desconfianza y prudencia ante todas las situaciones, además de la educación

G DATA | SIMPLY SECURE

G DATA ENDPOINT PROTECTION BUSINESS

SOFTHARD
Intelligent Safety