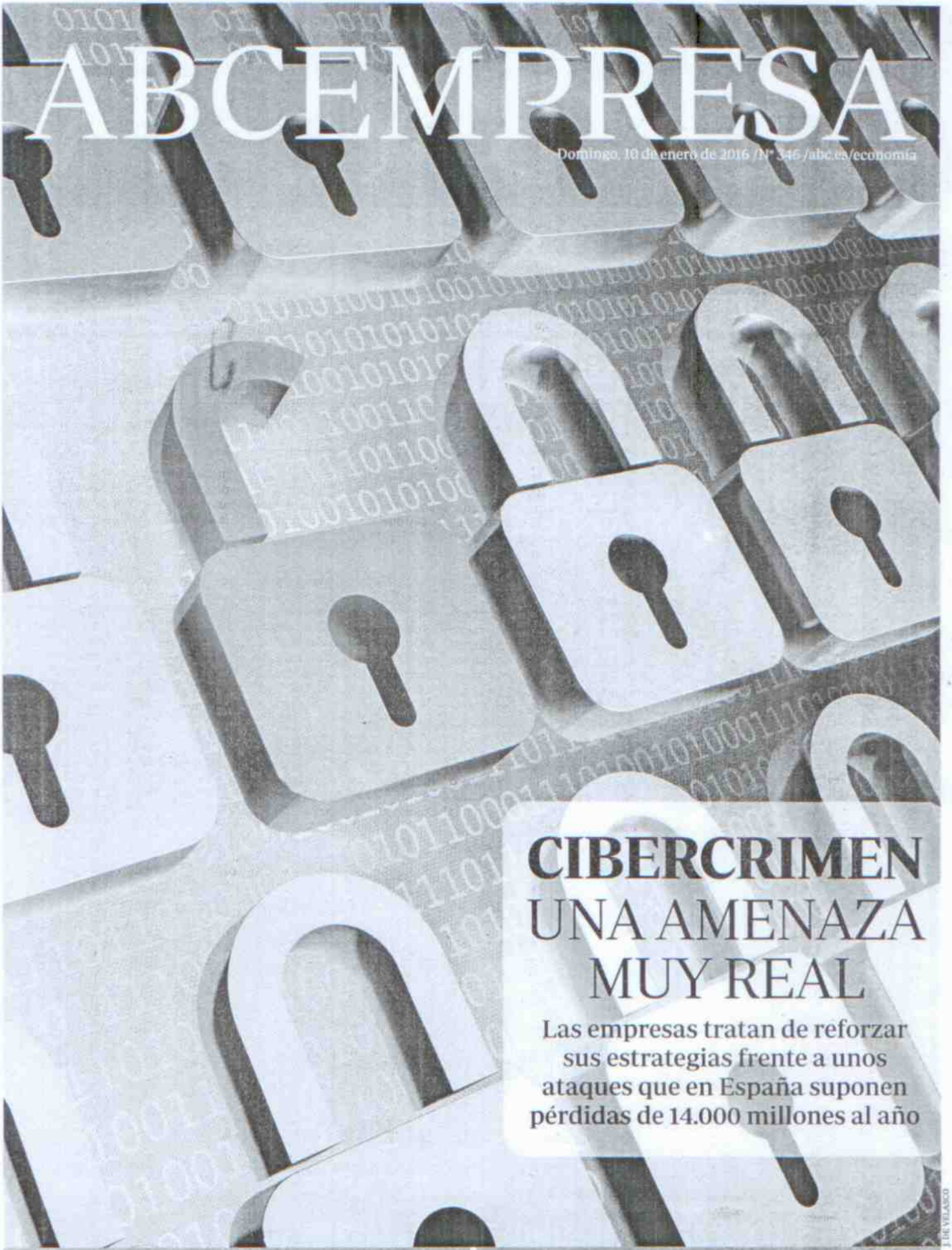
ABCEMPRESA
Domingo, 10 de enero de 2016 /Nº 346 /abc.es/economía



CIBERCRIMEN
UNA AMENAZA MUY REAL

Las empresas tratan de reforzar sus estrategias frente a unos ataques que en España suponen pérdidas de 14.000 millones al año

J. DE VELASCO

La banca europea se entrena a fondo para poder cumplir con las nuevas exigencias del BCE (8)

Una nueva era para el automóvil: los grandes del motor se suben al transporte colaborativo (10)

Cibercrimen las empresas se

En España, solo en 2015 se registraron 45.000 amenazas, que causaron pérdidas por valor de 14.000 millones de euros, el 1,4% del PIB

Los expertos censuran la heterogeneidad de los diferentes modelos jurídicos nacionales, que dificulta la persecución de los cibercriminales

UNAI MEZCUA

El 15 de agosto de 2012 la mayor parte de los 55.000 empleados de la principal petrolera del planeta, Saudi Aramco, celebraban en sus casas una de las festividades más sagradas del islam, la Noche del Destino, cuando se cree que Mahoma reveló el Corán a sus discípulos. Fue entonces cuando un grupo hasta entonces desconocido de «hackers» aprovechó para devolverla a la Edad de Piedra.

En cuestión de horas, millones de archivos desaparecieron y 35.000 ordenadores dejaron de funcionar. Los técnicos lograron evitar que el ataque afectase a la extracción del crudo, pero durante los siguientes meses, en lugar de ordenadores, impresoras y servidores, los trabajadores de la empresa que satisface el 10% de las necesidades mundiales de crudo tuvieron que recurrir de nuevo a bolígrafos, máquinas de escribir y faxes. ¿Cómo pudo suceder algo así?

«La mayoría de los grandes ciberataques se producen por una acción humana», asegura Alfonso Mur, socio director de servicios de seguridad de Deloitte. En el caso de Aramco, un «inocente» email que en realidad resultó ser una elaborada trampa en la que «picó» un empleado fue el detonante. Como descubrieron demasiado tarde los técnicos saudíes, cualquiera puede servir de caballo de Troya para los enemigos digitales de la empresa, que son muchos y cada vez más implacables.

Desnudos ante la amenaza

Según datos del banco de inversiones Julius Baer, en 2014 se registraron 42,8 millones de incidentes de ciberseguridad en todo el mundo, un 48% más que el año anterior y un 1.158% más que en 2009. Los responsables de buena parte de este incremento son las mafias organizadas especializadas en el mundo digital, cuya proliferación en los últimos años también ha hecho mella en España, donde solo en 2015 se detectaron cerca de 45.000 ciberataques, que causaron pérdidas de unos 14.000 millones de euros, equivalente al 1,4% del PIB.

Más preocupante que el número de ataques es, si cabe, constatar lo desprotegidas que están las empresas ante ellos. «El 51% de los ordenadores del mundo han experimentado virus o "malware"», explica Alfonso Mur, que destaca que las herramientas de protección habituales cada vez son más ineficaces: «El cien por cien de los atacados tiene "firewall" y un antivirus actualizado, y aún así, la mayoría no llega ni siquiera a enterarse de que han penetrado sus defensas». Prueba de ello es que, de media, una empresa tarda 205 días en detectar que ha sido atacada, según la consultora Mandiant. Cuando finalmente lo hace, en el 92% de las ocasiones no es el equipo encargado de la seguridad el que da el aviso, sino un cliente enfadado, un contratista o alguna otra persona o compañía externa, con el consiguiente daño en su reputación e imagen corporativa.

Ni siquiera los gigantescos departamentos de seguridad informática de las grandes multinacionales, con millones de euros de presupuesto, logran ser totalmente eficaces; ya que cada vez más deben combatir en un campo de batalla que está fuera de su perímetro defensivo: los dispositivos de sus clientes. Para los delincuentes resulta igual de rentable atacar uno por uno a los millones de clientes de una gran empresa, e infinitamente más sencillo, al no tener que sortear la sólida muralla digital que éstas suelen mantener en torno a sus activos. Por el contrario, los internautas promedio rara vez tienen instaladas barreras eficaces de protección, por lo que en el 75% de las ocasiones un «hacker» apenas tarda unos minutos en hacerse con el control de su máquina.

Nuevas armas

Para proteger y orientar a empresas, clientes e internautas, en 2014 se creó el Instituto Nacional de Ciberseguridad (Incibe), un organismo público dependiente del Ministerio de Industria cuya principal misión es operar un centro de respuesta a incidentes de ciberseguridad llamado CERT. Según explica su director general, Miguel Rego, el Incibe no solo pretende establecer una barrera protectora, sino que también trata de forma activa de evitar nuevos ataques colaborando con grandes y pequeñas empresas, a las que enseña a detectar los incidentes y a subsanarlos de forma gratuita. También facilita a las pequeñas y medianas empresas herramientas sin coste alguno, así como kits de formación y de sensibilización para los empleados.

El Incibe también es un órgano clave en materia de colaboración con otras administraciones, tanto españolas como internacionales. «El ciberespacio es un ente que no tiene fronteras y para poder prevenir incidentes y neutralizar a los atacantes se requiere colaboración nacional e internacional».

▸▸▸

Una lacra, pero también un negocio

U. M.

Como respuesta a la delincuencia digital en los últimos años se ha desarrollado un pujante negocio de alto valor añadido: el de la ciberseguridad. Según la consultora Gartner, el gasto en esta materia crecerá durante los próximos cuatro años un 80%, hasta los 65.000 millones de dólares anuales, en parte por la introducción de cada vez un mayor número de dispositivos conectados a internet, desde coches hasta marcapasos, que pueden ser «hackeados».

Por su parte, el banco de inversión Julius Baer recuerda que el Foro Económico Mundial ha listado las ciberamenazas como uno de los cinco riesgos más preocupantes para la seguridad mundial. El banco estima que las empresas deberán aumentar sensiblemente su inversión en ciberseguridad en los próximos años, por lo que considera que el sector presenta un gran atractivo, si bien «aún está muy fragmentado, lejos de la madurez y presenta una alta volatilidad».

En España, según datos de Incibe, la industria engloba a unas 130 empresas que emplean a unos 25.000 trabajadores de alta cualificación. Miguel Rego, director general de Incibe, asegura que las expectativas laborales son elevadas, puesto que el sector crece anualmente a un ritmo del 11%, y espera que siga haciéndolo por encima de los dos dígitos al menos hasta 2020. Entre las empresas punteras en nuestro país destacan multinacionales como Indra o Telefónica, pero también compañías más pequeñas como Panda, S21Sec o Nemo, que ya se han convertido en referentes fuera de nuestras fronteras.

Las pymes, presa fácil

El cibercrimen no debe ser solo una preocupación de las grandes compañías. Cualquier empresa, desde una ferretería de barrio con una base de datos de clientes hasta una cadena de supermercados de tamaño medio con sus sistemas informatizados puede ser víctima de un ciberataque y, de hecho, lo es. Según datos de la firma de seguridad informática Symantec, en 2015 las empresas

arman contra la guerra virtual

de tamaño pequeño y medio acumularon un 59% de los ataques de «spear phishing» –un correo electrónico que aparenta ser de una persona o empresa conocida pero cuyo objetivo es robar información o introducir un virus o troyano– como el que dejó fuera de combate a Saudi Aramco. Marina Nogales, directora de K2 Intelligence, cree que las pymes españolas «deben cambiar de mentalidad», puesto que no siempre toman las protecciones adecuadas frente a las ciberamenazas al considerar, erróneamente, que no pueden ser objeto de un ciberataque. «El 50% de las empresas ya han sido atacadas, y el otro 50% lo van a ser», asegura tajante.

Por su parte, Miguel Rego, director general del Instituto Nacional de Ciberseguridad (Incibe), distingue entre tres tipos de pymes: aquellas cuyo negocio depende de la tecnología, están bastante concienciadas, por lo que destinan mucho esfuerzo y presupuesto a su protección; en segundo lugar, las que tienen una dependencia media (utilizan internet y las nuevas tecnologías pero su negocio no gira en torno al comercio electrónico), con un nivel de ciberseguridad «manifiestamente mejorable»; y por último, las pymes que no utilizan prácticamente las TIC, entran en internet solo a modo de consulta y cuyo nivel de ciberseguridad es «bajo». Según Rego, los tres grupos son objetivo de los cibercriminales, en especial de ataques de extorsión por causa de malware que secuestra sus archivos y pide a cambio un rescate. Por ello, el Incibe ha puesto a su disposición en su web (www.incibe.es/) herramientas gratuitas y materiales para mejorar su conocimiento y formación. Ofrecen también un servicio de alerta temprana, avisándoles de nuevas amenazas que pueden llegar a afectarles. Además, planean lanzar en breve un servicio de herramientas especializadas por tiempo limitado a empresas con baja penetración de las nuevas tecnologías, con el objetivo de mostrarles los quebraderos de cabeza que una buena protección les puede evitar. «Es necesario convencerlas de que tienen que empezar a consumir productos de seguridad», concluye.

▸▸▸

explica Rego. Incibe mantiene contacto permanente con otros agentes españoles, como el Ministerio del Interior y en menor medida el mando conjunto de ciberdefensa del Ejército, así como internacionales, como con la Organización de Estados Americanos. También forman parte de una red internacional de centros de respuesta antiincidentes, «First», que mantiene reuniones periódicas en las que los organismos de los distintos países miembros comparten herramientas y experiencias.

Rego apunta también como problema la debilidad del derecho fundamental para perseguir a los ciberciminales, así como la heterogeneidad de los distintos modelos jurídicos nacionales. De forma similar lo percibe el juez de la Audiencia Nacional Eloy Velasco, codirector del programa de innovación en ciberseguridad de la Universidad de Deusto, un curso de alto nivel que pretende formar a directivos, emprendedores y altos responsables públicos y privados y concienciarlos de los riesgos de no protegerse debidamente de los delincuentes digitales.

«Los ciberdelitos han proliferado porque son el tipo de delito más cobarde», asegura Velasco, en referencia al anonimato que protege al delincuente que actúa detrás de un ordenador. El magistrado, uno de los mayores expertos españoles en la lucha contra el cibercrimen, valora de forma positiva la reforma de la Ley de Enjuiciamiento Criminal (Lecrim) que entró en vigor el pasado 6 de diciembre. La revisión permitirá, entre otras cosas, que la Policía pueda intervenir herramientas como el popular servicio de mensajería WhatsApp, infiltrar agentes encubiertos en el marco de investigaciones online con capacidad para intercambiar o enviar archivos ilícitos o incluso utilizar «troyanos», un software malicioso que brinda a un atacante acceso remoto al equipo infectado y que es una de las principales herramientas de los cibercriminales. Además, la legislación obligará ahora a los operadores tecnológicos que gestionen datos a colaborar de forma obligatoria. La ofensiva legal contra los ciberdelitos se complementa con la última reforma del Código Penal, que entró en vigor el pasado 1 de julio y que recoge explícitamente amenazas como el ciberterrorismo, la estafa informática, el espionaje mediante las nuevas tecnologías o el blanqueo de capitales de forma telemática.

Legislación
La Policía podrá infiltrarse en sitios web y enviar «troyanos»

Investigación
La ciudad israelí de Tel Aviv se ha erigido en La Meca de la ciberseguridad

Guerreros de élite

Estas herramientas, sin embargo, pueden no ser suficientes cuando los atacantes tienen un elevado nivel de sofisticación, los daños son demasiado cuantiosos o la información sustraída es en extremo delicada o la empresa atacada decide mantener el ataque en el más estricto secreto. En muchos casos las compañías prefieren no denunciar y recurren a compañías de élite que ayuden a evaluar los daños, contenerlos y evitar que se vuelvan a producir en el futuro.

En España, una de las empresas que ofrecen ese tipo de servicios es la consultora K2 Intelligence. Su rama de defensa en el ciberespacio emplea, entre otros, al ex agente especial encargado de ciberseguridad del FBI, Austin P. Berglas, encargado de desarticular el supermercado del crimen virtual Silk Road en 2013, y a antiguos miembros de los servicios de inteligencia de Israel, cuya segunda mayor ciudad, Tel Aviv, es considerada el «Silicon Valley» de la ciberseguridad. «Nuestro equipo está compuesto por profesionales que hablan más de veinte idiomas, entre ellos, chino o iraní, frecuentes entre los delincuentes ciberneticos», explica su directora en España, Marina Nogales, para cuya compañía nuestro país supone un gran foco de interés ya que, según sus cálculos, se trata del tercero más atacado por los delincuentes.

Los servicios de K2 Intelligence comienzan con la realización de un «penetration test», es decir, un ciberataque simulado sin previo aviso para detectar posibles fallas en sus defensas virtuales. Si la empresa no lo supera —y rara vez lo hace—, realizan un estudio pormenorizado de la compañía de varios meses de duración, que incluye rastrear la red para detectar posibles amenazas o filtraciones de archivos.

Una técnica que también emplea Deloitte, cuyo centro de operaciones de ciberseguridad para todo el mundo, CiberSOC, se sitúa en la localidad madrileña de Alcobendas. «El principal activo de defensa es "escuchar" lo que dicen sobre tí», coincide Alfonso Mur, quien asegura que la vigilancia constante que el equipo desarrolla en la red ha ahorrado más de un suceso desagradable a sus clientes e incluso a la propia auditora.

Pese a su cada vez mayor sofisticación y recursos, las empresas del sector todavía están muy lejos de poder asegurar que el digital es un entorno totalmente seguro para hacer negocios. Las más de 130 empresas que lo forman en España, junto con otras miles en todo el mundo, descubren día a día nuevas vulnerabilidades y se ven obligadas a actualizar constantemente sus técnicas para no quedar rezagados frente a los delincuentes mejor armados y más implacables de la Historia. Sin embargo, su constante innovación, su imaginación y su creciente experiencia son las mejores armas para evitar que, en un futuro cercano, sea usted quién se descubra recuperando de algún almacén polvoriento su fax y su vieja máquina de escribir.

Incidentes de ciberseguridad que afectan a ciudadanos y empresas registrados hasta diciembre
45.000

El cibercrimen provoca pérdidas del **1,4%** *del PIB de España. Más de* **14.000** *millones de euros al año*

FUENTE: INCIBE (Instituto Nacional de Ciberseguridad)/Julius Baer/Mandiant M-Trends

Protección Barreras contra los ciberdelincuentes

Consejos básicos de «higiene digital» para dificultar un ciberataque

U. M.

Los expertos confirman que unas sencillas prácticas reducen sensiblemente el riesgo de ser atacado. Eso sí, recuerdan que, como en cualquier otro ámbito, el sentido común es la mejor defensa.

Usar contraseñas seguras

Las contraseñas deben tener más de ocho caracteres e incluir caracteres alfanuméricos, es decir, combinar números y texto en mayúsculas y minúsculas. «De esta forma, hasta el ordenador más potente de la NASA tardaría cientos de años en descifrarla», explica Alfonso Mur, de Deloitte.

Actualizar el software

Constantemente, las compañías desarrolladoras detectan nuevas amenazas y publican «parches» con los que taponar posibles fallos, por lo que tener instalada la última versión puede ahorrar más de un disgusto. Esto también incluye no ignorar los avisos del sistema, por mucho que en ocasiones nos resulten molestos.

Evitar las memorias USB

Los expertos desaconsejan rotundamente utilizar memorias USB, en especial si han llegado hasta nuestras manos en forma de presente corporativo. En numerosas ocasiones, los conocidos popularmente como «pinchos» contienen malware capaz de infectar nuestro equipo y enviar información clave a otro dispositivo. Los expertos también sugieren evitar en lo posible trabajar en la nube, puesto que en este caso la información se almacena en servidores remotos cuya vigilancia y protección puede estar fuera del control de nuestra empresa.

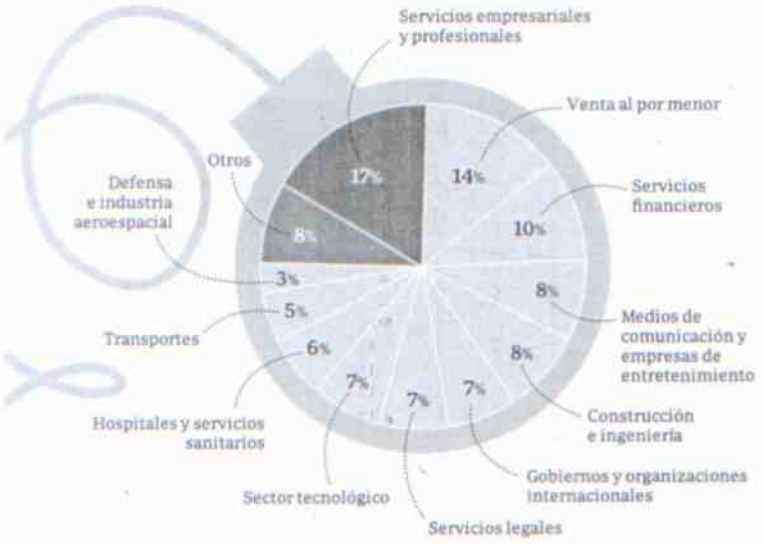
No hacer click sobre enlaces

Escribir manualmente las direcciones web a las que queramos acceder en lugar de clicar en un enlace que hayamos recibido por correo puede evitarnos acceder a un sitio web infectado o que haya sido diseñado por los delincuentes para imitar aquel que en realidad queríamos visitar.

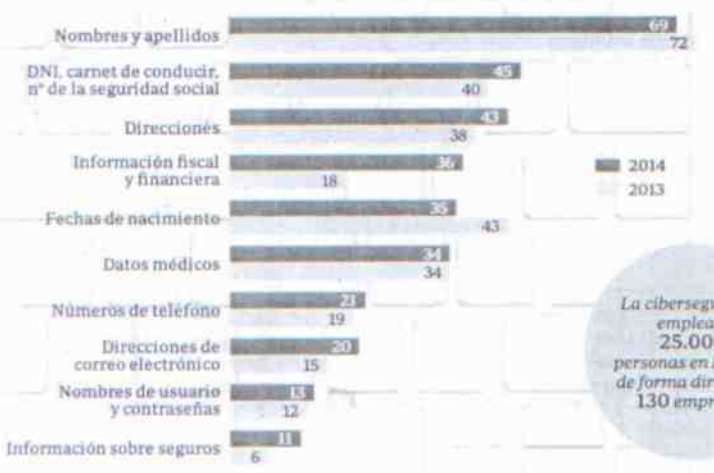
No usar Wi-Fi público

Las redes Wi-Fi, en especial si no son de confianza, pueden ser fácilmente atacadas para extraer información muy valiosa de nuestro dispositivo, como nuestras ubicaciones de acceso de los últimos años, o de los sitios

Sectores que registraron ciberataques en 2014



La información más vulnerada por los cibercriminales



La ciberseguridad emplea a **25.000** *personas en España de forma directa en* **130** *empresas*

ABC

web a los que accedamos a través de ella, como contraseñas y números PIN.

Cerrar siempre la sesión

Al acabar nuestra tarea, conviene cerrar completamente la sesión en el ordenador. De lo contrario, el equipo queda totalmente desprotegido y listo para cualquier otra persona de la empresa que decida realizar actividades ilícitas y encubrir sus movimientos entre los nuestros.

Utilizar el email corporativo

Utilizar nuestra cuenta de email personal para asuntos laborales puede causar un grave problema de seguridad, como bien sabe la candidata demócrata a la Casa Blanca, Hillary Clinton, que está siendo investigada por no utilizar la cuenta que le correspondía como secretaria de Estado. Los expertos lo desaconsejan no solo porque quedan fuera de la monitorización de la empresa, sino porque los correos enviados a través de gestores externos no pueden ser usados para auditorías o procesos judiciales. Además, sus condiciones de uso habitualmente les facultan para leer y procesar los contenidos que envíes a través de ellos.

Hacer copias de seguridad

Si todo lo demás falla y los «hackers» roban nuestros datos o los corrompen, la mejor solución para evitar tener que empezar de cero es poder recuperar con rapidez todo el trabajo anterior. Para ello, la mejor solución es realizar con frecuencia copias de seguridad y guardarlas en distintos lugares, por si alguna de éstas también se vieran comprometidas o dañadas por los atacantes.

Compartir, la mejor defensa posible

GIANLUCA D'ANTONIO PRESIDENTE DE ISMS FORUM SPAIN

Sin lugar a duda, 2015 ha sido el año de la ciberseguridad. Muchas empresas españolas se han enfrentado, algunas por primera vez, a este nuevo tipo de amenazas que el uso de las nuevas tecnologías ha traído consigo. Malware como «Cryptolocker» ha supuesto un desafío, hasta ahora desconocido por muchas organizaciones, capaz de poner en riesgo la misma continuidad del negocio.

Después de años de avisos, informes de Europol y de otros organismos internacionales, finalmente las amenazas se están materializando de forma constante también en el sector empresarial español. Llegado este momento, la pregunta que tenemos que hacernos es: ¿Estamos preparados?

> «Para hacer frente a los crecientes riesgos solo hay un camino: el de la colaboración público-privada»

La respuesta es difícil, el grado de madurez y preparación es diferente según el tamaño de la empresa, el sector de actividad, la cultura y los precedentes. Por tamaño, las grandes organizaciones pueden invertir y disponer de equipos especializados para hacer frente a las amenazas del ciberespacio. Estas capacidades, en las medianas y pequeñas empresas, solo pueden adquirirse a través de servicios externos. El sector de actividad también es relevante ya que determinados aspectos, como la regulación y el nivel de exposición al riesgo, o las incidencias sufridas, dependen de aquel. En esta óptica, se puede comprender la mayor preparación del sector financiero con respecto a los demás.

Sin embargo, factores como la cultura y los precedentes pertenecen al entorno particular y casi histórico de cada organización y, en definitiva, a su propensión al riesgo. Hasta hoy, la mayoría de los esfuerzos y, por ende, de las inversiones realizadas en estos aspectos, se han centrado en la prevención de los ataques y de los consecuentes incidentes de seguridad. Por contra, ante la eventualidad de un ataque exitoso, muchas organizaciones carecen de las capacidades necesarias para identificar la tipología de acciones maliciosas, detener las consecuencias dañinas y restaurar sus sistemas. Este conjunto de capacidades que los expertos identifican como ciber-resiliencia debe ser la prioridad para aquellas organizaciones que aspiren a gestionar de manera eficaz y eficiente la ciberseguridad de sus infraestructuras tecnológicas.

Para hacer frente a la creciente exposición a este tipo de riesgos, solo hay un camino, el de la colaboración público-privada donde la palabra «compartir» sea la guía maestra para alcanzar la ciber-resiliencia. La unidad de los actores involucrados, el intercambio de información, la puesta en común de las practicas exitosas..., son los elementos indispensables para hacer frente a las nuevas formas de criminalidad organizada que han visto en el cibercrimen una nueva forma de llevar a cabo sus actividades ilícitas. En este sentido, la reforma de la Ley de Enjuiciamiento Criminal que entró en vigor el pasado 6 de diciembre supone un ulterior paso adelante en la correcta dirección para luchar contra los nuevos tipos de delitos relacionados con el uso de las nuevas tecnologías. Ejemplo de ello es una nueva regulación específica para los denominados «agentes encubiertos informáticos», que con autorización judicial podrán infiltrarse en las redes y foros digitales. También la posibilidad de poder llevar a cabo, de forma remota, registros de equipos informáticos, ayudará a los investigadores policiales.

Con todo esto, 2016 se prefigura como un año de profundos cambios, en el cual la ciberseguridad se impone como una prioridad para todas aquellas organizaciones que quieran mitigar los riesgos relacionados con el uso del ciberespacio. España aprobó en 2013 su primera Estrategia de Ciberseguridad Nacional. Tras dos años, podemos constatar cómo los avances realizados en este ámbito están sirviendo de palanca para afianzar el uso de las nuevas tecnologías en todos los estrados de la Sociedad.

Iniciativas de concienciación como los simulacros organizados por ISMS Forum (CiberMS_2015), los Ciber-Ejercicios del sector privado de Incibe, o macro eventos como CyberCamp, ponen de manifiesto el compromiso de todos los actores para impulsar y fortalecer una cultura de seguridad que incluya las nuevas tecnologías y el ciberespacio como un ámbito de interés determinante. Actores de ámbito público-privado como ISMS Forum, el Instituto Nacional de Ciberseguridad o el Consejo de Ciberseguridad Nacional constituyen «el cortafuego» necesario para proteger los intereses españoles en el ciberespacio.

ISMS FORUM SPAIN ES LA ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN