Ciberdelincuentes: La gran amenaza

MARÍA ÁNGELES CABALLERO VELASCO
Subdirección General de Seguridad y Medio Ambiente MAPFRE

La tecnología ha crecido a pasos agigantados desde que nacieron los primeros ordenadores de usuario en los años 80, como el *Spectrum*, hasta los sistemas más sofisticados de los que podemos disponer hoy en día, desde dispositivos móviles que nos permiten estar conectados en cualquier parte del mundo hasta el "Internet de las Cosas", objetos de la vida cotidiana interconectados entre sí a través de la Red. La proliferación de las redes sociales, el incremento del consumo de servicios Web y la revolución de la nube o *cloud*, han potenciado todavía más la nueva era de dispositivos interconectados.

Este nuevo escenario ha provocado que usuarios, empresas y gobiernos cambien su comportamiento, su forma de interactuar con el medio. Hoy en día las empresas son completamente dependientes de las Tecnologías de la Información (TI). No se concibe que una empresa no se apoye en la tecnología para su correcto funcionamiento, siendo así los equipos de TI y su seguridad, una pieza clave en las organizaciones. ¿Se imagina una ciber-catástrofe que pudiera afectar a varios sectores y múltiples compañías al estilo "Jungla de Cristal 4.0"? Esto provocaría la interrupción de sus actividades y el robo o daño de sus sistemas informáticos, que en algunos casos podrían tener efectos directos frente al estado de bienestar de un país (centrales nucleares, empresas energéticas, etc.). Se ha estimado que si se paraliza la actividad de las compañías durante una semana podría llegar a tener un impacto económico de hasta 10 billones de dólares[1].

El auge de la tecnología que estamos viviendo en las últimas décadas, lleva asociado un incremento del riesgo tecnológico, en especial en los últimos años, debido principalmente a que ha puesto a disposición de los ciberdelincuentes un nuevo mundo de fraude con la consecuente creación de nuevas formas de llevar a cabo delitos a través de la tecnología. Esta situación ha provocado en las empresas una creciente preocupación llevando a éstas a la creación de equipos especializados dedicados exclusivamente al control y supervisión de estos riesgos (los llamados *blue-team*), llegando incluso a la respuesta ante posibles incidentes de seguridad.

Para poder comprender esta situación desarrollaremos brevemente el concepto del **riesgo** desde una perspectiva empresarial, medido como el producto de las amenazas, vulnerabilidades y su impacto sobre el negocio. El riesgo lo podemos entender como los escenarios posibles que pueden comprometer la totalidad o parte de los recursos de una empresa, poniendo en peligro la viabilidad de ésta. Como contrapeso a este riesgo las empresas consecuentemente deben establecer las medidas adecuadas para mitigar, evitar, traspasar o aceptar estos riesgos. Expondremos qué **amenazas** nos acechan en la Red y más adelante las **contramedidas** para paliar y gestionar dichas amenazas.

CIBERAMENAZAS, FRAUDE Y DELITOS EN LA RED

Los "tipos malos" reinventan cada año nuevas formas de llevar a cabo delitos telemáticos, pero también es cierto que existen algunas constantes que llevan repitiéndose a lo largo de los años y algunas de ellas han ido en decremento. Por ejemplo, el *spam* ha caído un 50% en una década de acuerdo con el último *Intelligence Report* de Symantec.

Los ataques más populares tienen como objetivo tanto servidores empresariales como dispositivos de usuario final. Los ataques físicos están comenzando a ser menos comunes pero los ataques sociales se han incrementado en los últimos años. Las **principales ciberamenazas**[2] a las que se enfrentaron las compañías en el pasado año se pueden describir a través de nueve patrones: ataques a páginas Web (35%), ciberespionaje (22%), intrusión en puntos de venta al cliente (14%), copia ilegal de tarjetas de crédito (9%), mal uso de sistemas por empleados internos (8%), software malicioso o *malware* (4%), errores misceláneos (2%), robo o pérdida física (<1%) y ataques de denegación de servicio (<1%). Se calcula ya para este año 2015 que las pérdidas económicas que sufrirán las empresas europeas sobrepasarán los 14.000 millones[3] de euros a causa de los ciberataques y estos ataques, no sólo tienen un carácter económico sino también reputacional. Cabe destacar que España es el tercer país con más ciberataques del mundo, tras Estados Unidos y Reino Unido. Veamos en qué consiste cada uno de éstos ataques.

[CIBERESPIONAJE Y CIBERGUERRA]

El **ciberespionaje** no sólo afecta a gobiernos o administraciones públicas, sino también a empresas privadas. Los llamados ataques dirigidos o APTs (*Advanced Persistent Threat*) se diseñan específicamente para una entidad concreta y uno de sus principales objetivos es el de conseguir información confidencial de las compañías, con un fin monetario o de espionaje industrial y/o político.

En el pasado 2012, Saudí Aramco, la mayor petrolífera del mundo, sufrió uno de los peores ataques[4] de **ciberespionaje industrial** en la historia de la ciberseguridad. Alrededor de 30.000 ordenadores y unos 2.000 servidores quedaron inaccesibles en cuestión de horas. El ataque se inició a través de un correo electrónico que contenía un enlace que descargaba un software malicioso, el cual se expandiría por el resto de la Red silenciosamente para atacar de manera simultánea durante el Ramadán, cuando la mayoría de los empleados de la empresa se encontraban de vacaciones. Saudí Aramco se embarcó de nuevo en el mundo del papel y del fax y no fue capaz de controlar la compra/venta de petróleo durante meses decidiendo al cabo de un tiempo regalarlo para no parar la producción, con las consecuentes pérdidas millonarias que esto supuso para la empresa. El ataque se lo auto-atribuyó el grupo *"Cutting Sword of Justice"* el cuál hizo mención del apoyo de Saudí Aramco al régimen político de la familia real de Arabia Saudí.

En el caso de la guerra cibernética o **ciberguerra**, que va más allá del mero espionaje industrial, tenemos el ejemplo de "Stuxnet". En el 2010, Stuxnet salió a la luz, conocido en su momento como el *malware* más inteligente jamás creado y fue desarrollado para los sistemas industriales de tipo SCADA. Se ideó con el fin de atacar a las centrales nucleares ubicadas en Irán, consiguiendo ralentizar en 10 años la fabricación de uranio enriquecido en dichas centrales. Se cree, por los indicios encontrados en el código fuente, que fue desarrollado en conjunto por EEUU e Israel, y con una duración de más de un año de tiempo llevado a cabo por un equipo de expertos, no se trataba de ningún juguete desarrollado por un mero aficionado.

[MALWARE]

En el caso del malware o software malicioso podemos distinguir entre las variantes que intentan hacerse pasar por un programa "legítimo" tratando de suplantar la identidad de alguna entidad y las variantes que restringen el acceso a determinadas partes del sistema operativo, cifrando sus ficheros y pidiendo un rescate a cambio, el cuál se conoce técnicamente como ransomware (del inglés ransom, rescate y ware, software).

Un ejemplo de malware de suplantación de identidad sería el conocido como "virus de la policía", del que hablaremos más adelante en el apartado de Ingeniería Social. Respecto a la segunda variante ¿quién no ha sufrido o conoce de alguien al que se le ha infectado su dispositivo con un "virus" que ha cifrado todos sus ficheros y que no le permite hacer ninguna acción en su sistema? El **malware** tipo cryptolocker está siendo unos de los peores quebraderos de cabeza para los equipos de seguridad y soporte a usuario en las empresas. Los equipos de operaciones deben de estudiar todo el ciclo de infección, desde que el malware se recibe (habitualmente por correo electrónico) hasta su detección y una vez que los sistemas se han infectado, puesta en cuarentena y corrección mediante recuperación de copias de seguridad o backups del sistema, ya que algunos de estos "virus" son prácticamente imposibles de eliminar y hay que restaurar el sistema a un estado previo. Otra opción que tenemos para eliminarlo es pagando a los "tipos malos" pero de ésta manera estaríamos colaborando directamente con el cibercrimen.

Este tipo de fraude se conoce como **Crimeware,** el hecho de comprometer sistemas de usuario o servidores mediante software malicioso, incluyendo el *phishing*. A través de portales Web aparentemente confiables, los "tipos malos" buscan datos de usuarios, contraseñas, información de pago, etc. Tienen como objetivo suplantar la identidad de una organización (habitualmente sites bancarios) con el fin de obtener una recompensa económica. En ocasiones los ataques son muy sofisticados, pero en otros casos son fáciles de detectar.

Por ejemplo, existe una variante de éste tipo de *phishing*, donde se le pide al usuario todos los números de la tarjeta de coordenadas bancarias y depende de la ingenuidad de la víctima el picar o no en el anzuelo.

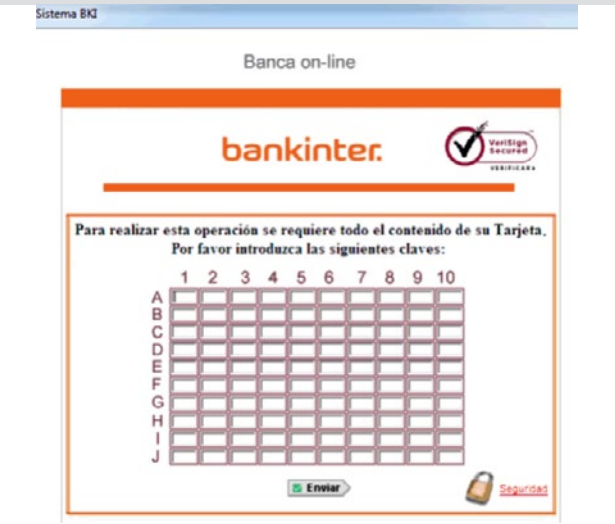


Ilustración 1. Ejemplo de *Phishing* Bancario

[TPVS Y COPIA TARJETAS CRÉDITO]

Cuando hablamos de ataques a **Puntos de Venta (TPV) o *Point of Sales* (PoS)**, los atacantes tratan de comprometer servidores o los dispositivos PoS con el objetivo de obtener información de pago. Las empresas que más sufren este tipo de ataques son las de ventas al consumidor de a pie como las del sector de hostelería. Otra amenaza relacionada es la instalación de terminales falsos en los cajeros automáticos para robo de tarjetas de crédito, lo que afecta principalmente a entidades bancarias.

Para evitar éste tipo de fraude, Visa y MasterCard diseñaron una norma de obligado cumplimiento (PCI-DSS) con el objetivo de aumentar la seguridad de los datos y de las operaciones realizadas con tarjetas de crédito, la cual afecta a todas aquellas compañías (y comercios) que procesan, transmiten y/o almacenan dichos datos.

[PÁGINAS WEB]

Los **ataques a páginas Web** se basan principalmente en comprometer credenciales de usuario mediante fuerza bruta o robo y/o en explotar vulnerabilidades en el software o infraestructura que soporta dicha aplicación Web, como por ejemplo los gestores de contenidos o plataformas de comercio electrónico. La mayoría de las empresas ponen a disposición de sus clientes y sus empleados plataformas Web necesarias para el negocio pero que pueden poner en riesgo la información de la empresa.

[DENEGACIÓN DE SERVICIO]

En los últimos años las compañías han sufrido numerosos **ataques de Denegación de Servicio Distribuidos,** conocidos como DDoS (del inglés, *Distributed Denial of Service*). En las noticias habremos oído hablar de ataques de organizaciones *hacktivistas* como Anonyumus o LulzSec que han dejado sin conectividad o inhabilitado una página Web de una compañía. Habitualmente se consigue a través de ataques DDoS y con el objetivo de lograr un daño reputacional. Para la ejecución de este ataque se infectan un gran número de ordenadores conectados a la Red para obtener suficientes recursos y lograr que el ataque sea exitoso. De esta manera forman lo que se denomina una *botnet* o una red de ordenadores infectados o *bots*. En el momento del ataque se hace uso de todas las máquinas infectadas para generar un inmenso número de conexiones simultáneas hacia un objetivo concreto, la página Web de la compañía en cuestión.

[FUGA DE INFORMACIÓN]

La fuga de información es una de las amenazas más críticas para una organización. El **mal uso** de los sistemas de la organización y sus datos, la **pérdida de dispositivos** o de información impresa, la falta de control de acceso en las instalaciones o los **errores misceláneos** (como podría ser divulgar datos privados en una red pública o enviar un correo electrónico a destinatarios equivocados) podrían comprometer la información de la organización. Sin una adecuada gestión de estas amenazas, podríamos incurrir en graves multas cuando se trata de datos de alto nivel de seguridad ante las normativas de protección de datos, como por ejemplo datos personales o de salud.

INGENIERÍA SOCIAL

Uno de los mayores retos planteados a los equipos de seguridad de la información de las empresas es la **ingeniería social**. Las técnicas de ingeniería social manipulan al usuario a través de la psicología y las habilidades sociales del atacante para obtener de la víctima la información que desea, que variará entre conocer cuál es su usuario y contraseña, conseguir acceso a zonas restringidas u obtener dinero a cambio de algo que nunca llegará. Las técnicas de ingeniería social cada vez son más sofisticadas y más difíciles de detectar. Los cibercriminales ya no necesitan desarrollar aplicaciones complejas, si no que se centran en la persona, que es el eslabón más débil de la cadena desde el punto de vista de seguridad. Los cibercriminales confían en la manipulación psicológica para estimular a la víctima a hacer cosas que habitualmente no haría, obteniendo de ellos información verdaderamente valiosa.

Muchos de los ataques comentados previamente como el *cryptolocker* o el *phishing* bancario son ejemplos de *malware* que hace uso de técnicas de ingeniería social. Un ejemplo de ello es el que se ha popularizado como "virus de la policía". Éste tipo de virus trata de impresionar a sus víctimas haciéndoles creer que han cometido un delito (propiedad intelectual, pornografía, pederastia, *copyright*, etc.) y pone amablemente a disposición de éstas un método de pago fácil y sencillo para solventar el delito que "ha cometido".

Ilustración 2.Virus de la policía

Estos ataques son muy difíciles de paliar ya que implican directamente a las personas. La mejor **contramedida** al respecto es la divulgación, concienciación y formación de los usuarios para que conozcan de la existencia de éste tipo de técnicas y sean capaces de defenderse.

LOS "TIPOS MALOS" Y SUS VÍCTIMAS

¿Y quiénes son estos **"tipos malos"**? Son los nuevos cuatreros de la Red, mafias organizadas provenientes de todo el mundo, cuyo *malware* tiene su origen esencialmente en países del este de Europa y países asiáticos que se dedican a la creación de este tipo de software con el objetivo de obtener información o dinero de manera ilícita. La labor de las Fuerzas y Cuerpos de Seguridad del Estado se hace muy complicada para atrapar estos tipos malos que juegan en esencia con dos factores: **distancia/fronteras y anonimato en la Red.** En ocasiones operan a través de "mulas" o "muleros" que no son más que meros intermediarios que hacen el "trabajo sucio". Estas mafias organizadas, contratan a personas a través de ofertas de trabajo haciéndoles creer que van a cooperar en planes estratégicos de multinacionales y que pueden conseguir dinero de forma fácil y rápida. Su trabajo viene a ser el de transportar la mercancía o el dinero de un sitio a otro, de ésta manera se pierde la trazabilidad y se complica la búsqueda de los tipos malos.

No todos los atacantes son mafias organizadas, muchos de los ataques se producen por **personal interno**, conocidos como *insiders*, que conocen y dominan el escenario, por lo que el ataque puede ser mucho más dañino que cuando se trata de actores externos. Por otro lado también encontramos el perfil del ***hacktivista*** que comentábamos previamente, motivados por una ideología concreta, realizan ataques con un determinado fin. Por último, nos encontramos con otro tipo de perfil cuando hablamos de ciberguerra, como son por un lado los **Estados** y por otro los **terroristas.** Las **víctimas** de estos ataques podríamos ser nosotros mismos. Todas las industrias y negocios están en riesgo, aunque pensemos que el riesgo de ataque externo no es elevado, siempre existirá el riesgo de un ataque interno o de que los usuarios hagan mal uso de los sistemas y expongan información sensible al público. Lo cierto es que el público objetivo ha mutado de las grandes empresas a las PYMES o pequeñas y medianas empresas, lo que está elevando el número de ciberataques de manera exponencial. Se observan ataques desde entidades y administraciones públicas hasta sectores como el farmacéutico, el hotelero o la venta al por menor.

El año pasado se superó el número de ciberdelincuentes en más de 70.000, los cuales provocarán pérdidas, como comentábamos al principio del artículo, de más de 14.000 millones de euros en este 2015. Podemos afirmar que la ciberdelincuencia mueve más dinero que el narcotráfico[5] en los últimos tiempos.

¿Y por qué los llamamos "tipos malos" cuando popularmente se conocen como "hackers"? Cabe decir que la palabra *hacker* se ha desvirtuado con el paso del tiempo, lo que se venía conociendo en los años 80 como personas habilidosas con los ordenadores las cuales eran capaces de hacer cualquier cosa con ellos por diversión hoy en día se les asocia con "piratas informáticos", como introdujo la RAE en Octubre del 2014. En su día, dicha acepción provocó duras críticas por el colectivo de expertos en seguridad al no asociarlo también a su significado en origen. Sería más correcta la denominación de *cracker* o *ciberdelincuente.*

QUÉ PUEDO HACER PARA GESTIONAR EL RIESGO EN MI COMPAÑÍA

El combatir las principales ciberamenazas a las que nos enfrentamos en tiempo y forma, puede suponer un elemento diferencial y definitivo en la continuidad y sostenibilidad de nuestro negocio. Es necesario definir una estrategia proactiva, en lugar de actuar sólo cuando los accidentes pasan. Antes o después nuestra empresa va a ser atacada.

El riesgo por su propia naturaleza no se puede eliminar, pero sí podemos desarrollar contramedidas para reducirlo, tanto a nivel jurídico, organizativo como medidas de carácter más técnico. El éxito en la reducción del riesgo al que nos vemos expuestos pivota entre dos **pilares: gobierno y seguridad tecnológica**, por un lado tenemos el marco normativo, legal y jurídico, establecer adecuadas políticas de seguridad y buenas prácticas en las compañías y por otro la seguridad tecnológica. El fin que persiguen dichos pilares básicos es el de la protección de los activos de la compañía, destacando a "las personas", como el activo más importante.

Respecto al **gobierno de la seguridad**, debemos tener en cuenta varios factores. Es imprescindible conocer en primer lugar el apetito del riesgo de la empresa, y ponerlo en contexto con el marco legal y jurídico del país: normativas asociadas a la protección de datos, normativas relacionadas con el ciberterrorismo, normativas de salud y financieras o de nuestro sector de actividad. En la misma línea, debemos establecer en nuestra compañía adecuadas políticas empresariales y de seguridad, así como en el desarrollo de un código de conducta e invertir en divulgación y concienciación, para que todos los usuarios de la compañía sean conocedores de dichas normativas. Un estudio de *Enterprise Management Associates*, destacó que sólo el 56% de los empleados había recibido algún tipo de formación en seguridad, protocolos o políticas.

En el ámbito de la **seguridad tecnológica** diferenciamos entre la seguridad lógica o de la información y la seguridad física. Debemos de trabajar dentro de nuestra compañía en aspectos clave, como manejar una adecuada infraestructura de seguridad, instaurar un adecuado equipo de respuesta a incidentes y disponer de adecuados controles de seguridad física en las instalaciones de nuestra compañía. Los equipos de respuesta a incidentes dan servicio a través de Centros de Operaciones de Seguridad y se constituyen como CERT's (*Computer Emergency Response Team*) como parte de la Red de CSIRT's mundiales (*Computer Security Incident Response Team*). Algunos de los más conocidos a nivel nacional son el CCN-CERT del Centro Criptológico Nacional o el CERT de Seguridad e Industria operado por INCIBE_ (Instituto Nacional de Ciberseguridad), que trabaja para la protección de las infraestructuras críticas nacionales y la lucha contra los ciberdelitos y ciberterrorismo, entre otros. Este tipo de instituciones a nivel gubernamental (existentes en otros países) centran su labor esencialmente en la salvaguarda del estado del bienestar del país. En España, en particular, las actividades realizadas por estos centros se enmarcan dentro de la **Estrategia de Ciberseguridad Nacional**.

Como última recomendación destacaríamos que es imprescindible estar al día en seguridad, no sólo los equipos expertos, sino todos los empleados de una compañía. Los usuarios de la organización, deben de conocer los riesgos a los que se ven expuestos y la capacidad para gestionar éstos riesgos de una u otra manera. Uno de los productos que está proliferando en las empresas son los **seguros en materia de ciberseguridad** que tratan de dar una respuesta ante un desastre cibernético y reputacional. Una vez que se han minimizado los riesgos, el riesgo residual que queda latente se transfiere a través de pólizas específicas de ciberriesgos. Destacaríamos el famoso caso de SONY del 2011, en el que se llegaron a robar más de 25 millones de cuentas que contenían alrededor de 18 mil tarjetas de crédito y cuentas bancarias a través de la *Play Station Network*.

En definitiva hay que diseñar una estrategia de seguridad continua, persistente, y sostenible, disponer de sistemas e infraestructuras actualizados e invertir coherentemente en ciberseguridad para asegurar las infraestructuras de la compañía, garantizar el éxito y la continuidad de nuestra compañía.

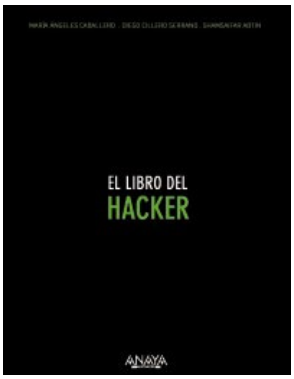
MAPFRE Y SU APORTACIÓN EN EL MUNDO DE LA SEGURIDAD DE LA INFORMACIÓN

MAPFRE, como empresa comprometida con la sociedad, trabaja continua y activamente en la protección de los intereses de sus clientes, empleados, accionistas y proveedores, mediante la prevención y detención de incidentes de seguridad.

Este trabajo continuo se lleva a cabo a través de su equipo de expertos en ciberseguridad de la Dirección Corporativa de Seguridad y Medio Ambiente y su Equipo de Respuesta a Incidentes de Seguridad de la Información conocido como el CCG-CERT. El equipo de respuesta a incidentes de MAPFRE dispone de un sofisticado laboratorio y un grupo de profesionales altamente cualificados con el cometido de prevenir, responder y minimizar el impacto de posibles incidentes de seguridad. En el contexto global y multinacional de MAPFRE la labor del CCG-CERT no es meramente interna, si no que colabora activamente con otras compañías e instituciones tanto a nivel nacional, como internacional.

BIBLIOGRAFÍA RECOMENDADA: EL LIBRO DEL HACKER DE ANAYA

Si desea iniciarse en el mundo de la seguridad de la información o profundizar en la materia del artículo, le recomendamos **El Libro del Hacker** de la editorial ANAYA. En el libro se abordan cuestiones de seguridad, desde capítulos introductorios a la in-seguridad de la información hasta las técnicas de ataque más sofisticadas, desde sus primeras fases (*footprinting/fingerprinting*) pasando por sus etapas más avanzadas (*exploiting*) y borrado de evidencias. También podemos encontrar otros temas de actualidad como seguridad en redes sociales, *cloud computing*, gestión de identidades, ciberamenazas, etc.



Se trata de un libro que puede ayudar tanto a personas que estén interesadas en introducirse en el mundo de la seguridad de la información como a expertos algo más avanzados. En la página Web de la editorial se puede consultar su ficha para más información: http://www.anayamultimedia.es/libro.php?id=3608921 ■

[1] "Cyber Catastrophe" *working paper, University of Cambridge Judge Business School*

[2] "Verizon Data Breach Investigation Report" (DBIR) – 2014

[3] "España, a la cabeza del cibercrimen" Diario ABC – 2015

[4] "Arabia Saudí dice que el ataque informático contra Aramco fue lanzado desde el exterior" El País http://economia.elpais.com/economia/2012/12/09/agencias/1355069609_526898.html

[5] La ciberdelincuencia mueve más dinero que el narcotráfico en el mundo http://www.abc.es/espana/20141207/abci-ciberdelincuencia-dinero-201412062106.html