CIBERCRIMINALIDAD
Noviembre 2021

I. INTRODUCCIÓN.

La cibercriminalidad se ha convertido en uno de los fenómenos delictivos con mayor crecimiento en España.

Prueba de ello es que el último *Estudio sobre la cibercriminalidad en España*, publicado por el Ministerio del Interior en 2020, señala que aquel año se registraron un total de 287.963 hechos delictivos relacionados con las tecnologías de la información y las comunicaciones, lo que suponía un incremento de un 31,9% con respecto al año anterior. Los fraudes informáticos representaron un 89,6% de los delitos detectados en este ámbito. Las empresas constituyen una de las víctimas predilectas de esta forma de delincuencia. Así, recientemente se estimaba en un 25% el crecimiento mundial de ciberataques a empresas durante la pandemia.[1]

Al creciente número de casos se suman las dificultades a la hora de investigar y perseguir estos delitos. Al respecto, el estudio antes mencionado destaca que solamente el 14% del total de los hechos registrados en 2020 fueron esclarecidos.

Ante este escenario, el objetivo de la presente *Newsletter* es ofrecer un breve análisis de este fenómeno delictivo, así como proporcionar algunas pautas básicas para prevenir y reaccionar a tales ilícitos.

II. BREVE RELACIÓN DE CIBERATAQUES MÁS FRECUENTES.

Para empezar, y sin ánimo de exhaustividad, se ofrece una breve relación de las modalidades de ciberataques más comunes:

- ***Phishing:***

En el *phishing* encontramos a un sujeto —el *phisher*— que, con la finalidad de obtener determinada información confidencial (como contraseñas, número de tarjeta de crédito, etc.), envía un mensaje o correo electrónico a la víctima suplantando la identidad de una persona u organización de su confianza (como un banco, un colegio profesional, una aseguradora, etc.), solicitándole que realice con urgencia una acción determinada y advirtiéndole de que,

[1] https://www.lavanguardia.com/economia/20210503/7424172/ciberataques-empresas-crecen-25-causa-pandemia.html

BARCELONA
C/ Balmes nº 76, 4-1, 08007, Barcelona
Tel. +34 93.171.02.73 - Fax +34 93.171.02.74
rgva@rgva.es www.rgva.es

MADRID
C/Monte Esquinza nº 34, bajo B, 28010, Madrid
Tel. +34 91.576.78.37 - Fax +34 91.578.31.12
rgva@rgva.es www.rgva.es

de no hacerlo, las consecuencias serán negativas.

El mensaje suele incluir un enlace a una página web fraudulenta, que imita la de la persona u organización suplantada, donde la víctima debe realizar la acción solicitada o donde se infecta su equipo con un archivo malicioso.

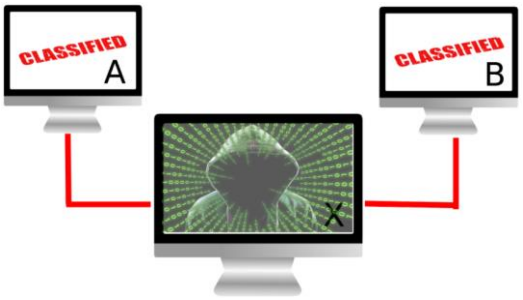
- ***Pharming:***

Es una variante de la modalidad anterior que se basa en la manipulación del tráfico de un sitio web para redirigir a los usuarios a sitios web falsos, pero que imitan la apariencia del auténtico, y que instalarán *software* malicioso o registrarán los datos personales de la víctima, como sus contraseñas o información bancaria.

Hay dos modalidades básicas: en la primera, el ciberdelincuente previamente habrá instalado un virus u otro programa malicioso en el equipo de la víctima, que la desviará del sitio que desea visitar a otro que es falso, pero que imita al auténtico. En la segunda, se infecta el servidor DNS de la propia página web de la institución de confianza (banco, universidad, etc.), de forma que los usuarios que intentan acceder a ella son redirigidos al sitio web falso. Esta última modalidad es más peligrosa, pues no requiere haber infectado previamente el equipo del usuario y permite llegar a un mayor número de víctimas.

- ***Man in the middle:***

En este caso, el ciberdelincuente intercepta una comunicación entre dos o más interlocutores, sin que estos se percaten. Ello le permite conocer el contenido de la comunicación y modificarla a su antojo, suplantando la identidad del interlocutor legítimo, para a continuación dejar que el mensaje siga su camino.



Fuente: INCIBE

Por ejemplo, el ciberdelincuente puede interceptar un correo en el que un vendedor proporcione sus datos bancarios a un comprador y cambiar los datos por los suyos propios, consiguiendo así que el comprador haga una transferencia a una cuenta equivocada.

- ***Ransomware:***

Mediante un programa malicioso se infecta un equipo para secuestrar información y luego extorsionar a la víctima solicitando dinero para recuperar los datos. Para infectar el equipo existen varias técnicas, siendo una de las más

frecuentes el envío de correos de *phishing* con archivos o enlaces maliciosos.

- ***Spoofing:***

El acto de suplantar la identidad es lo que conocemos como *spoofing*. Los ciberdelincuentes utilizan para ello diversas técnicas, como falsificar los *email headers*, esto es, la parte del correo electrónico que ve el receptor del mismo y donde se encuentran las direcciones del emisor y del receptor, los servidores por los que el mensaje ha pasado, la fecha de envío, el asunto, etc. De esta forma se consigue engañar a la víctima, que creerá que se comunica con alguien de confianza.

Para dar aún más credibilidad al engaño, en ocasiones los ciberdelincuentes adjuntan a esos correos documentos oficiales falsificados, como certificados bancarios o notas registrales.

III. TRATAMIENTO PENAL DEL FENÓMENO.

El fenómeno de la ciberdelincuencia es complejo y se manifiesta de formas muy diversas. Ello implica que no haya un delito que nos permita abarcar todos los casos, sino que, dependiendo de la dinámica comisiva, deberá procederse a adaptar las figuras delictivas tradicionales a las necesidades específicas del caso. Con todo, pasamos a enumerar a continuación cuáles son los principales delitos que los Juzgados y Tribunales aprecian en estos casos:

- **Estafa**
- **Daños informáticos**
- **Contra la intimidad**
- **Pertenencia a organización criminal**
- **Usurpación de funciones públicas**
- **Intrusismo**
- **Falsedad documental**
- **Blanqueo de capitales**

IV. POSIBILIDADES DE REACCIÓN.

Como ya se ha avanzado en la introducción, la investigación de los ciberdelitos no es tarea sencilla. Frecuentemente no se detectan a tiempo, lo que retrasa la reacción y agrava las consecuencias. Otras veces no podrá determinarse con certeza dónde se ha producido la brecha de seguridad y, por ello, cuál es el alcance de la vulnerabilidad.

Una complicación añadida radica en que la Policía no da traslado de las actuaciones a la autoridad judicial si en 72 horas desde la denuncia no identificado a sospechosos. Por ello, si quiere acudir a la vía judicial, normalmente la víctima tendrá que reiterar la denuncia ante el Juzgado de Instrucción

o la Fiscalía, o directamente interponer una querella.

Además, los bancos, amparándose en la normativa sobre protección de datos, no suelen proporcionar información sobre los titulares de las cuentas a las que se transfiere el dinero, en caso de que esta haya sido la dinámica comisiva empleada. Esto es especialmente relevante a la hora de identificar a las denominadas "mulas", sujetos que, sin haber participado del ciberdelito, reciben en su cuenta bancaria el dinero detraído, para posteriormente transferirlo a otras cuentas (a cambio de una comisión) o sacarlo en pequeñas cantidades.

Las dificultades para detectar e investigar estos delitos comportan graves problemas a la hora de intentar recuperar el dinero. Pese a la multiplicidad de métodos delictivos posibles, nos centraremos aquí en aquellos que implican una transferencia bancaria a la cuenta directa o indirectamente controlada por los ciberdelincuentes.

Al respecto, es evidente que la primera opción sería actuar contra los autores del ciberdelito para exigirles su responsabilidad civil. Sin embargo, habitualmente estos cubrirán bien su rastro o bien no se encontrarán en España, sino que actuarán desde servidores extranjeros, lo que dificultará su identificación y persecución. Más sencillo suele ser acabar identificando a las mencionadas "mulas", aunque estas posiblemente sean insolventes, lo que, de nuevo, dificulta conseguir el resarcimiento.

En consecuencia, una alternativa puede ser tratar de reclamar la responsabilidad civil del banco por su intervención en la mencionada operación de transferencia. Las expectativas de éxito entonces varían en función de la casuística. Así, no será posible obtener resarcimiento alguno de los bancos en caso de transferencia conscientemente efectuada a los delincuentes, aunque haya sido bajo coacción (caso de *ransomware*). En cambio, mucho más sencillo será apreciar la responsabilidad civil del banco si estamos ante un caso de *pharming* a través de una vulnerabilidad en el servidor DNS de su página web. Por supuesto, en este caso, como en todos los relacionados con la ciberdelincuencia, disponer de un buen peritaje informático será esencial.

En el resto de casos en los que se pretenda el resarcimiento por parte del banco, las cosas no son sencillas, pues debe tenerse en cuenta que, en el orden civil al menos, la posición de la entidad bancaria está bastante protegida. Así, el Real Decreto-ley 19/2018, de servicios de pago, dispone en su art. 59 que cuando una orden de pago se ejecute por la entidad bancaria de acuerdo con el identificador único

proporcionado por el ordenante, se considerará correctamente ejecutada en relación con el beneficiario especificado en dicho identificador. Es decir, que si el IBAN de la cuenta de destino coincide con el proporcionado por el ordenante, aunque no coincidan los beneficiarios, los bancos quedan exentos de responsabilidad.

Esto dificulta sumamente obtener el resarcimiento del daño por parte del banco en casos en los que la víctima efectuó la transferencia a una determinada cuenta bancaria debido a un engaño de los ciberdelincuentes, pese a que en su orden de transferencia indicara un beneficiario distinto al titular de la cuenta de destino.

No obstante, como decimos, la jurisprudencia civil es sumamente restrictiva a la hora de apreciar la responsabilidad de los bancos. Para que ello ocurra, considera necesario que concurran, cumulativamente, los siguientes requisitos:

Que el banco careciese del consentimiento del ordenante.

Que el ordenante no cometiera ningún fraude.

Que el ordenante no actuara con negligencia grave.

Que el ordenante comunique la incidencia en cuanto la conozca.

A destacar, en este sentido, que si un usuario de servicios de pago niega haber autorizado una operación o alega que se ejecutó de forma incorrecta, el banco deberá demostrar que la operación fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por cualquier deficiencia. Esto puede servir para fundamentar una responsabilidad del banco en casos en que a un usuario le hurtan las claves de forma fraudulenta, si bien, en el caso concreto, será necesario determinar el nivel de diligencia de dicho usuario a la hora de protegerlas.

Dicho esto, lo cierto es que en el orden penal existe una temprana sentencia del Tribunal Supremo (2013) que se aparta del criterio antes explicado y considera que el banco de destino tiene el deber de comprobar no solo que coincide el IBAN, sino también el beneficiario indicado por el ordenante de la transferencia. Con todo, la jurisprudencia penal posterior se ha apartado mayoritariamente de esta opinión aislada, siguiendo el criterio restrictivo predominante en el orden civil, antes apuntado.

En este contexto, y más allá de resaltar la razonabilidad de la mencionada sentencia de nuestro Alto Tribunal, una vía adicional a explorar para conseguir que los bancos respondan sería tratar de explotar eventuales incumplimientos en materia de prevención del blanqueo de capitales, lo

que abriría la posibilidad —de momento, aún remota— de conseguir que las entidades bancarias en que se constataran dichos incumplimientos tuvieran que sufragar los perjuicios civiles derivados.

V. RECOMENDACIONES.

Ante un ataque informático, es importante reaccionar con rapidez y denunciarlo sin demora a la Policía. En este sentido, recomendamos pre-redactar la denuncia con ayuda de un experto para que su contenido sea completo y no se perjudique la posición jurídica de la víctima en una eventual reclamación posterior. Téngase en cuenta, además, que para cualquier gestión con los bancos estos pedirán que se aporte la correspondiente denuncia policial. Ello sin perjuicio de que, como se ha dicho anteriormente, ante un previsible estancamiento de la investigación policial pueda interponerse una querella.

Sin embargo, las dificultades antes expuestas para investigar estos delitos y recuperar el dinero distraído aconsejan que los esfuerzos se centren, en la medida de lo posible, en una buena prevención. Las siguientes recomendaciones pueden ayudar a reducir el riesgo de sufrir un ataque o a paliar sus consecuencias.

i. Establecer protocolos de empresa.

En concreto, son especialmente recomendables estas dos medidas:

a) Designar a un responsable.

Es recomendable designar a una persona (o a varias, dependiendo del volumen de la empresa) encargada de gestionar las entradas y salidas de caja. Con ello, se consigue reducir el número de personas que pueden disponer del dinero de la empresa, y coherentemente el número de posibles víctimas de engaño, centralizando en una o pocas personas los riesgos de sufrir una estafa. El responsable asumirá un especial deber de cuidado al realizar las transferencias, debiendo cumplir con una serie de protocolos.

b) Definir protocolos de actuación.

Ya se ha comentado la facilidad con la que los ciberdelincuentes pueden suplantar identidades o falsificar certificados bancarios. Establecer unos simples protocolos puede ser de gran utilidad.

Por ejemplo, si se recibe un email de un cliente anunciando un cambio de cuenta, una simple llamada al remitente para verificarlo puede evitar el engaño.

Asimismo, debe desconfiarse de mensajes escritos con faltas ortográficas, en un idioma distinto del habitual o que exigen realizar una determinada acción con urgencia. Y, por supuesto, nunca deben abrirse enlaces ni correos procedentes de fuentes desconocidas.

Por último, mencionar que en casos de *ransomware*, el Instituto Nacional de Ciberseguridad (INCIBE)[2] recomienda no pagar nunca el dinero exigido, pues es frecuente que los ciberdelincuentes posteriormente exijan nuevas cuantías o que repitan el ataque al saber que la víctima está dispuesta a pagar.

ii. Mejorar la seguridad informática.

A mayor seguridad, menor riesgo de ser víctima de un ataque. Un buen modo de empezar con la mejora de la seguridad puede ser aplicando un Plan Director de Seguridad (PDS)[3], que consiste en hacer un análisis del nivel de seguridad inicial de la empresa para, a continuación, establecer un conjunto de medidas para reducir los riesgos de sufrir un ataque hasta unos niveles aceptables.

Asimismo, existen herramientas que permiten reducir el riesgo de ataques. En el ámbito de los correos electrónicos fraudulentos, por ejemplo, una de las más eficaces es el DKIM *(Domain Keys Identified Mail)*, que permite al receptor de un correo electrónico comprobar que procede realmente del remitente y que no ha sido modificado tras el envío.

Otras medidas sencillas y recomendables son tener siempre actualizado el *software* de los equipos (especialmente el sistema operativo y el navegador), proteger los equipos con contraseñas robustas de difícil adivinación y no conectarse a redes wifi abiertas.

Para más información sobre estos sistemas, u otros igualmente eficaces, recomendamos consulten a su informático de referencia.

iii. Contratar seguros especializados.

Ante el auge de los ciberdelitos, las compañías aseguradoras han empezado a diseñar seguros específicos para paliar las consecuencias de un ciberataque.

Estos seguros, conocidos como 'seguros de ciberprotección' o 'seguros ciberriesgo', permiten cubrir tanto la responsabilidad civil de la empresa frente a terceros como parte de las pérdidas económicas derivadas del ataque.

Para más información en materia de seguros, recomendamos consultar a vuestra compañía aseguradora.

Quedamos a su disposición para cualquier aclaración o comentario que pudieran precisar en relación con esta *Newsletter*.

* * *

[2] Para más información: https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

[3] Para más información: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

BARCELONA

C/ Balmes nº 76, 4-1, 08007, Barcelona
Tel. +34 93.171.02.73 - Fax +34 93.171.02.74
rgva@rgva.es www.rgva.es

MADRID

C/Monte Esquinza nº 34, bajo B, 28010, Madrid
Tel. +34 91.576.78.37 - Fax +34 91.578.31.12
rgva@rgva.es www.rgva.es