Expansión | JURÍDICO

¿Están preparados los bufetes para rechazar un ciberataque?

Los despachos de abogados están en el punto de mira de los 'hackers'. El secuestro de datos relevantes de los casos que llevan con el fin de obtener un rescate ('ransomware') es el ataque más habitual.

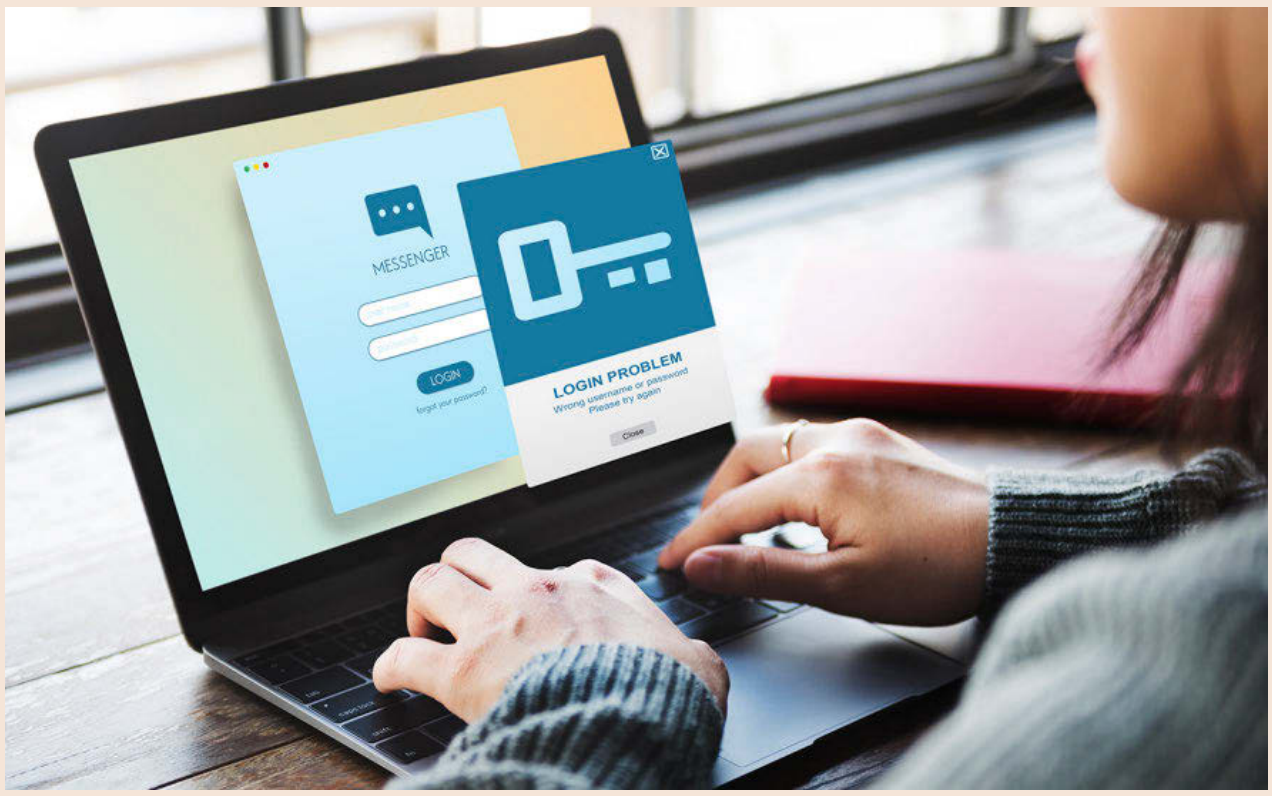
Salvador Carrero. Bilbao

El tipo de información que manejan y el hecho de que haya muchas firmas pequeñas que tienen menor protección informática, ha provocado que, en los últimos años, los bufetes se hayan convertido en un objetivo preferente de ciberataques. Según el Instituto Nacional de Ciberseguridad (Incibe), durante 2016 se reportaron en España al menos 70 ataques de *ransomware* a despachos de abogados. Estas situaciones, aparte de importantes pérdidas económicas, pueden tener graves consecuencias para la reputación corporativa.

Pero, ¿están actualmente protegidos los despachos frente a un ciberataque? Jesús Yáñez, socio de Ecija, considera que "la progresiva digitalización de los bufetes está haciendo que éstos sean conscientes de la necesaria implementación de sistemas para garantizar la seguridad de su infraestructura".

Asegura el letrado que sortear ciberataques depende en gran medida de tener implementado en el despacho un sistema de gestión de la seguridad de la información sólido, basado en estándares internacionales, el cual puede ejecutarse por la propia firma o por un tercero que le preste servicio. Estar preparado ante un ciberataque no supone sólo lidiar con posibles incidencias, sino "gestionar íntegramente la seguridad de los sistemas del despacho: servidores, ordenadores, portátiles, dispositivos móviles como *smartphones*, aplicaciones, bases de datos y, por supuesto, formación expresa a los usuarios de estos sistemas", destaca.

Álvaro Fernández de Araoz, director de desarrollo de negocio de Mr. Houston, entiende que la formación en seguridad es uno de los puntos débiles de los despachos y debería abordarse como un valor estratégico en su gestión. "La cuestión no es si nos atacarán o no, sino cuándo lo harán, cómo lo va a aguantar nuestra organización y, si hay discontinuidad de negocio, cuánto vamos a tardar en estar operativos de nuevo". Lo que se está viendo, asegura este experto, es que "si un ataque es expresamente preparado para una persona o entidad en concreto, es muy probable que tenga éxito".



Dreamstime

El 24% de los incidentes de ciberseguridad se origina por causas internas.

Desde una valoración aproximada, el departamento de seguridad de Mr. Houston considera que los despachos de más de 150 abogados están muy bien preparados frente a los ciberataques, pues disponen de un buen plan de seguridad, un compromiso de la dirección y formación y concienciación continua del personal.

Los bufetes de tamaño medio –50 a 150 abogados– tienen una buena protección, con personal técnico *in house* más concienciado y formado sobre ciberseguridad de la Red. Por último, estarían los despachos de menos de 25 abogados, donde existen más brechas de seguridad y, en general, están menos protegidos.

Los despachos de abogados con menos de 25 profesionales son los que están menos protegidos

En caso de brecha de seguridad, el bufete deberá comunicarlo a los clientes y a la autoridad competente

Responsabilidad legal

Los despachos de abogados están obligados a cumplir tanto las normas establecidas para la protección de datos, que están recogidas en el Reglamento General de Protección de Datos (RGPD) como las establecidas en el real decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Esta normativa no establece específicamente qué medidas deben implementarse o no, sino que éstas deberán ser escogidas por el bufete teniendo en cuenta el análisis de riesgos que se realice en interno.

No obstante, según apunta Yáñez, lo más recomendable es "atender a estándares internacionales como ISO 27001, NIST, o incluso en España al Esquema Nacional de Seguridad, que propone medidas de seguridad concretas a implementar para garantizar estas cuatro esferas de seguridad".

En materia de protección de datos, de existir una brecha de seguridad, el responsable será el despacho, que deberá comunicarlo a los clientes y a la autoridad competente. Además, el cliente podrá reclamar por daños y perjuicios.

Ataques más frecuentes

Según explica el departamento de seguridad de Mr. Houston, los ataques más frecuentes a los que se enfrentan los despachos son los realizados a través de *ransomware*, por medio de *phishing* y la infiltración en la Red por medio de infraestructura y software desactualizado.

En menor medida también se dan ataques de DDOS llevado a cabo por *hacktivistas* en despachos que llevan casos de gran repercusión social.

Otra variante que hay que destacar es la fuga de información causada por empleados o socios descontentos o que han sido despedidos, que pueden tomar represalias contra el despacho difundiendo documentos o datos a los que han tenido acceso.

Como comenta Fernández de Araoz, según su experiencia, el 24% de los incidentes en ciberseguridad en una firma se origina por causas internas, entre otras por el mal uso de *pendrives* infectados o dispositivos propios robados o perdidos.

TIPOS DE ATAQUE

'Ransomware'
Secuestro de datos, restringiendo el acceso a los archivos para exigir posteriormente un rescate en 'bitcoins' (criptomoneda no rastreable).

'Phishing'
Suplantación de la identidad de una compañía o servicio, normalmente a través de correo electrónico, pidiendo datos confidenciales a los usuarios, como contraseñas de cuentas bancarias, para su propio beneficio.

DDOS
Ataque de una red de ordenadores que colapsa un servidor al realizar un alto número de peticiones y que, por tanto, no permite su uso por los clientes.

MEDIDAS PARA PREVENIR UN ATAQUE

- Proteger los equipos, teniendo el sistema actualizado, un buen antivirus y 'antimalware'.
- Concienciar y formar a los trabajadores sobre el riesgo de ataque, pues se calcula que un 80% de los incidentes se debe a descuidos y errores humanos.
- Usar contraseñas fuertes. Lo ideal es combinar números, letras mayúsculas, minúsculas y símbolos.
- Comprobar la autenticidad de enlaces y perfiles, pues es bastante común recibir ataques de 'phishing' a través del correo electrónico, mediante el cual se intenta adquirir información confidencial de forma fraudulenta.
- Utilizar protocolos de seguridad para el envío de datos, lo que supone no mandarlos a través de fuentes desconocidas o sitios de poca confianza.
- Evitar contenidos desconocidos, ya que abrir emails y descargar archivos adjuntos es una de las principales fuentes de ataque.
- Realizar una copia de seguridad es una medida fundamental, pues siempre se podrá recuperar la información perdida o secuestrada.