Director General de Kalibo Correduría de Seguros

MIGUEL DE LAS MORENAS OROZCO

"Los ciberriesgos, no son exclusivos de las grandes empresas", "Un ataque cibernético puede poner en peligro uno de los activos más importantes que atesora una empresa, la información, tanto datos personales, como confidencial"

Las amenazas cibernéticas suponen una de las principales preocupaciones de riesgo para las empresas y en la era digital esta tendencia se está viendo incrementada. La pérdida de información contenida en un portátil, las amenazas que representa el cloud computing, una denegación de servicio, la desconfiguración de su red o interrupciones de su presencia en Web, suponen un ciberriesgo que puede provocar un importante daño a su negocio.

Todos estos elementos están inmersos en un entorno donde la regulación legal y sancionadora está en aumento, lo que obliga a las empresas a prepararse y tomar los pasos más adecuados para el análisis y transferencia de estos riesgos. De hecho, el aumento de estas amenazas ha hecho que la Unión Europea esté preparando un Reglamento, de obligado cumplimiento, que sustituya a la directiva de 1995 por la que las empresas estarán obligadas a demostrar la efectividad de sus modelos de seguridad.

Por situarnos, ¿qué es un seguro de ciberriesgos?

Se trata de una innovadora solución aseguradora diseñada para contrarrestar algunas de las consecuencias que producen tanto una violación de seguridad como una fuga de datos. Además como no todos los riesgos y empresas son iguales, hay una solución para cada una de ellas.

¿Cualquier empresa es susceptible de un ciberataque?

Efectivamente. Las empresas deben realizar el análisis de su exposición a estos riesgos si, entre otras características, almacenan información privada, tienen una alta dependencia en procesos electrónicos o redes, contratan con proveedores de servicios tecnológicos, dependen de o gestionan infraestructuras críticas como empresas logísticas, almacenamiento de archivo, … o, simplemente, les preocupan un posible acto mal intencionado por parte de la competencia o del propio personal de la empresa.

En caso de un ataque cibernético, ¿la empresa puede decidir que la noticia no sea pública?

La notificación de riesgos de violaciones de seguridad a los abonados o particulares afectados ya es una realidad de conformidad con la Ley General de Telecomunicaciones, pero el nuevo Reglamento Europeo de Protección de Datos lo hará extensivo a todas las empresas que ofrezcan bienes y servicios a los consumidores europeos, incluidas aquellas que tengan sus servicios fuera de la Unión.

Pero con los seguros tradicionales, ¿no existe la protección adecuada?

No existe ningún tipo de cobertura de responsabilidad cibernética ofrecida en otros tipos de seguros de responsabilidad civil. Los ciberriesgos tienen otras consecuencias fundamentales como pérdidas económicas directas, potenciales procedimientos e investigaciones regulatorias, así como un impacto directo en la reputación de la empresa, que depende en gran medida de la gestión de la crisis que acometa la organización tras el incidente.

¿Hasta dónde llega la actuación de la aseguradora?

El cliente cuenta con el apoyo de un equipo de siniestros ciber a nivel mundial, que comparten experiencias en violaciones de seguridad y privacidad que ocurren en cualquier lugar del mundo, lo que permite que este equipo se encuentre en primera línea de conocimientos y mejores prácticas. Son conocedores de la importancia de dar una rápida respuesta en la tramitación de asuntos relacionados con los ciber riesgos.

¿Qué hay que hacer en caso de que se produzca un ciberataque?, ¿con qué respaldo cuenta la empresa en caso de tener cobertura aseguradora?

En este tipo de riesgos tan novedosos, es muy importante que el cliente se sienta respaldado. Para ello, el equipo de siniestros de la aseguradora proporciona una respuesta inmediata para evaluar y controlar el impacto de una violación de seguridad, restablecer la operativa del negocio y a cubrir las responsabilidades legales.

Ante una brecha de seguridad, se produce una respuesta inmediata en menos de 1 hora por el asesor asignado a la empresa. Expertos forenses determinan hasta dónde ha llegado el daño, como ocurrió y cómo subsanarlo. Mientras tanto, expertos legales y de comunicación asesoran para mitigar el posible daño reputacional.

La aseguradora también cubre los gastos de notificación a los afectados ante un uso ilegítimo de sus datos personales, así como los gastos de defensa ante una inspección del regulador de protección de datos y el pago de una posible sanción.

Y el posible daño producido a un tercero, ¿también está cubierto?

Así es, por supuesto. La empresa cuenta con cobertura de gastos de defensa y perjuicios por el uso ilegítimo de datos personales, datos contaminados por virus, robos de códigos de acceso al sistema, actos negligentes o errores de empleados…

Por bajar al terreno práctico, dígame ejemplos de ciberataques que hayan ocurrido.

Ejemplos, lamentablemente hay múltiples. Un empleado de una compañía de atención al consumidor que robó información personal de miles de clientes. Un grupo de hackers logra acceder a los sistemas informáticos de una cadena hotelera con varios establecimientos. Un servidor de correo electrónico y el disco duro de una empresa son robados mientras se encuentran en posesión de un proveedor externo.

Íker Berges Angós. Abogado
ikerberges@gmail.com

Los programas de cumplimiento normativo pueden evitar la RESPONSABILIDAD PENAL de las empresas

Tal y como ya se ha ido señalando en este espacio, desde el año 2010, tras una profunda modificación del Código Penal, se introdujo, por primera vez en España, la responsabilidad penal de las personas jurídicas que implicaba que, desde ese momento, cualquier empresa, en la que cualquier persona que la integraba llevaba a cabo la comisión de un acto delictivo en provecho de la misma, directo o indirecto, podía ver cómo era condenada penalmente a cuantiosas multas, suspensiones de actividad o, incluso en el peor de los casos, a la disolución y liquidación forzosa de la misma.

Al mismo tiempo de la creación de la responsabilidad penal, el legislador otorgó un mecanismo a las personas jurídicas para que, dado el caso de la comisión de un acto delictivo dentro de la organización de la misma, pudiese verse exonerada de esta responsabilidad se había llevado a cabo cuantos actos hubiesen sido necesarios para evitar dicha actuación delictiva. De este modo, a partir de ese año 2010, comienzan a surgir los Programas de Cumplimiento Normativo o de Compliance Penal como mecanismo de organización interna de la empresa y, adicionalmente, como modo de exoneración de responsabilidad penal.

Pues bien, seis años después de la introducción de la responsabilidad penal de las empresas, el Tribunal Supremo ha dictado sus primeras sentencias en las que condenaba penalmente a entidades por haber sido beneficiadas por actuaciones delictivas llevadas a cabo por directivos o trabajadores. Tal y como queda perfectamente claro en las citadas resoluciones la falta de una Programa de Cumplimiento Normativo o de Compliance, la incorrecta implantación o la falta de actualización del mismo, ha resultado clave a la hora de que la empresa no se haya visto eximida de responsabilidad y ello debido a que el Tribunal ha entendido que esta dejación de funciones en cuanto a la elaboración o actualización de este instrumento ha devenido como esencial a la hora de poder evitar la comisión del delito.

Así, a modo de ejemplo, la Sentencia del Tribunal Supremo 154/2016 de 29 de febrero de 2016, establece en su Fundamento Jurídico 8° que: "Núcleo de la responsabilidad de la persona jurídica que, como venimos

diciendo, no es otro que el de la ausencia de las medidas de control adecuadas para la evitación de la comisión de delitos, que evidencien una voluntad seria de reforzar la virtualidad de la norma, independientemente de aquellos requisitos, más concretados legalmente en forma de las denominadas "compliances" o "modelos de cumplimiento" , exigidos para la aplicación de la eximente…"

En definitiva, la implantación de unos protocolos que prevean las posibles actuaciones delictivas dentro de una empresa y el establecimiento de las medidas necesarias para su evitación puede ser la frontera entre la vida y la desaparición de una empresa lo que, evidentemente, debería llevar a todas las personas jurídicas a evaluar la posibilidad de introducir estos instrumentos en su organización.