Cuándo, no si. La importancia de estar preparado para los ciberriesgos

Por Olivier Marcén, Head of Financial Lines, Insurance para Iberia en Sompo.

Originalmente publicado por Actualidad Aseguradora

La creciente perspectiva de un ciberataque es una de las principales amenazas en el radar de los profesionales del riesgo de todo el mundo. La frecuencia de los incidentes y sus posibles consecuencias son un importante motivo de preocupación para las empresas de todos los tamaños y de todos los sectores.

En España, el ciberriesgo está en el punto de mira de la mayoría de los gestores de riesgos, con un informe del Departamento de Seguridad Nacional que muestra que el número de ciberataques registrados en 2023 fue más del doble que en 2022, superando los 100.000 incidentes. Según Statista, una de cada seis infracciones penales registradas en España en 2023 fue un ciberdelito.

La ciberamenaza está evolucionando. Los piratas informáticos ya no son actores solitarios sino, cada vez más, parte de redes delictivas muy organizadas y con muchos recursos. No solo sus ataques son más selectivos, sino que los ciberdelincuentes actuales emplean nuevas técnicas y tácticas, como el uso de inteligencia artificial (IA) para crear vídeos falsos de gran profundidad con los que extorsionar rescates.

La concienciación sobre el riesgo cibernético es alta entre las empresas y los intermediarios en España. Las organizaciones cuentan con procedimientos y controles sólidos. Entre ellos, añadir parches, escanear continuamente y aplicar actualizaciones de seguridad; asegurarse de que la autenticación multifactor (MFA) está en funcionamiento; utilizar software de respuesta de detección de extremos (EDR) para proteger las estaciones de trabajo y los servidores; y garantizar que se realizan copias de seguridad offline de los sistemas, entre otras medidas.

En el caso de la cibernética, uno es tan fuerte como su eslabón más débil. Con demasiada frecuencia, las debilidades están dentro de la propia organización. Es importante que todos los miembros de la empresa, desde los más jóvenes hasta los más veteranos, conozcan los riesgos cibernéticos y sepan cómo responder a ellos. Y esta formación debe mantenerse al día para garantizar que todo el mundo sabe qué hacer si se produce un incidente cibernético.

Los gestores de riesgos también son muy conscientes de que no sólo hay que tener en cuenta el riesgo directo para su propia organización. En un mundo cada vez más interconectado, las empresas pueden verse afectadas por infracciones llevadas a cabo en proveedores y vendedores que puedan tener conexiones a sus sistemas y acceso a datos críticos, por ejemplo.

Es vital, por tanto, que las empresas se aseguren de que supervisan los sistemas de seguridad de los terceros con los que trabajan y confíen en la solidez de los protocolos de gestión de riesgos y protección que tienen implantados.

Pero incluso con los mejores protocolos de seguridad, nunca es posible estar protegido al 100% contra un ciberataque. Es una cuestión de cuándo se producirá un ataque, no de si se producirá. Los gestores de riesgos son conscientes de que, para minimizar los daños causados a las operaciones de su empresa por un ataque, necesitan un plan para gestionar un incidente y conseguir que los sistemas vuelvan a estar en línea y en funcionamiento lo antes posible.

Los planes de emergencia para la continuidad de la actividad en caso de ciberataque deben estar bien documentados y probarse y actualizarse periódicamente. No responder con rapidez a un ciberataque puede suponer un desastre financiero y de reputación para una empresa. Una póliza de seguro cibernético desempeña un papel importante en este caso, no sólo al proporcionar la transferencia del riesgo, sino también el acceso a la experiencia y los servicios que ayudan a las empresas a prepararse para los riesgos cibernéticos, tanto antes como después de un evento.

La adopción del ciberseguro es buena entre las grandes empresas y las multinacionales que operan en España. Sin embargo, actualmente es más desigual entre las pequeñas y medianas empresas (PYME), que representan más del 99% de todas las empresas que operan en la Unión Europea y alrededor del 99,9% de las empresas en España, según el Instituto Nacional de Estadística (INE).

Los datos de Telefónica Cyber Security Tech muestran que alrededor del 60% de las pymes españolas que sufren un ciberataque abandonan el negocio menos de seis meses después del incidente. El coste medio de un ciberataque a una PYME es de unos 35.000 euros, según los datos.

Es importante que el mercado asegurador demuestre a los compradores de PYME el valor real de una póliza cibernética y que trabaje con ellos para elevar el nivel de ciberseguridad en su empresa y en todos los sectores industriales. Esto implicará no sólo la cooperación entre sectores y el diálogo con corredores y otros expertos en seguros, sino también la colaboración con el Gobierno y los organismos de seguridad.

Se trata de una amenaza en constante evolución. Es vital que todos hagamos todo lo posible por contar con planes para evaluar, mitigar y gestionar el riesgo, transferirlo cuando sea posible y disponer de estrategias para recuperarnos después de un suceso.