Ciberseguros, también en el transporte

Cada día surgen nuevos peligros cibernéticos que difícilmente se pueden cuantificar mediante estadísticas o estudios. Robos de bases de datos, pérdidas de contraseñas, virus informáticos, correos electrónicos fraudulentos... son solo algunos de los riesgos a los que una empresa se ve expuesta. Según el INCIBE, el Instituto Nacional de Ciberseguridad, España es el tercer país del mundo en el que más ataques informáticos registran las empresas. En 2017, el 34% de las empresas en España sufrió una interrupción de sus operaciones y un 48% perdió información confidencial, mientras que en los primeros 6 meses de 2019 el dato del impacto de los ciberataques alcanza al 76% de las empresas, según una encuesta elaborada por la consultora Deloitte. Este escenario nos lleva a pensar que ya no debemos cuestionar si las Ciberamenazas pueden incidir sobre una empresa, la pregunta que tenemos que formularnos es cuándo sucederá y si contamos con los mecanismos adecuados para gestionar un Ciberataque.

En este contexto nacen los Cyberserguros, seguros pensados para **PROTEGER** y paliar a las **EMPRESAS Y AUTÓNOMOS** de los peligros cibernéticos.

Los incidentes más comunes son: virus informáticos (27%), ataques de ransomware (12%) y fraude en las transferencias bancarias por suplantación de identidad (10%). Evaluando el proceso de detección y gestión del incidente, las empresas reconocen que en el 50% de las ocasiones pasaron más de 3 horas hasta descubrir que habían sufrido el incidente. Solo en el 19% de los casos el problema fue descubierto antes de que pasara una hora. En 3 de cada 10 incidentes (33%) la compañía no recuperó su actividad normal hasta pasadas 8 horas tras la detención.

El último informe de HISCOX sobre sobre Ciberpreparación y referido al año 2019 concluye que el 43% de las empresas españolas dedicadas a la logísitica y tranporte ya tienen contratados sus cyberseguros.

En la mayoría de los casos de cyberataques en el sector del transporte están relacionados con colapsos de los sistemas informáticos, pérdidas de contacto con los vehículos controlados por GPS, robos de datos, tanto de clientes como de proveedores, información contable, etc

Las consecuencias de los ciberataques son de tres tipos:

1. En primer lugar, pérdidas económicas que se derivan del colapso de los procesos y los servicios;
2. Por otro lado, de un quebranto de la reputación y de la fiabilidad del operador.
3. Además, las empresas se enfrentan además a graves sanciones económicas por parte de la Administración.

Las garantías que ofrecen las compañías de seguros son diversas, pero básicamente centran en estos seis bloques.

- Asistencia informática preventiva
- Asistencia legal preventiva
- Asistencia informática post siniestro
- Asistencia legal post siniestro
- Responsabilidad Civil
- Pérdida de beneficios.

Conviene aclarar que no existe en la actualidad obligación legal alguna para contratar un seguro de este tipo. Si bien es cierto que, con la entrada en vigor el 25 de mayo de 2018 del Reglamento General de Protección de Datos (RGPD), tener un ciberseguro permitiría cumplir con alguna de las nuevas exigencias con mayor seguridad.

En el mercado hay bastantes aseguradoras que están especializándose en ciberseguridad. Consulte condiciones de esta tipología de seguro sin compromiso alguno en el Departamento de Seguros de Fundación GUITRANS Fundazioa .

Eduardo Lázaro Mendizabal

Gerente Correduría Lázaro San Juan
Departamento de Seguros
Fundación GUITRANS Fundazioa.