Ciberseguridad: mejor prevenir que curar

El pasado 20 de septiembre, la Autoridad Portuaria de Barcelona (APB) anunció a sus clientes que estaba siendo objeto de un ciberataque que había afectado a varios de sus servidores y que su departamento de Sistemas de la Información estaba valorando el alcance del ataque y actuando según el Plan de Contingencia preestablecido para estas situaciones. Poco después, la APB anunció que *«se había respondido activamente al ataque, operando con total normalidad y sin verse alterada en ningún momento su operativa marítima y terrestre»* y que se *«continuará trabajando hasta restablecer las funcionalidades, únicamente internas, que se han visto afectadas»*.

En una encuesta efectuada muy recientemente por BIMCO, a la que respondieron más de 350 personas del sector marítimo, más del 20% informaron de que habían sido objeto de ataques cibernéticos. De éstos, el 72% mencionaron que su propia compañía fue víctima de un incidente cibernético en los últimos 12 meses. Como conclusión, BIMCO considera que, *«los numerosos ataques e incidentes cibernéticos en los últimos doce meses indican que el sector debe prepararse mejor en este campo. En la encuesta, el 27% de los encuestados informaron de que nunca habían recibido formación sobre seguridad cibernética, sólo alrededor de la mitad de los encuestados tienen establecidos planes para asegurar la continuidad de su negocio, en caso de ser víctima de un ataque a la seguridad cibernética, y el 31% de los encuestados no tenía ninguno»*.

De hecho, de los encuestados por BIMCO que habían sido objeto de un ataque, el 49% reconocieron que, como consecuencia del mismo, se habían interrumpido sus servicios y que al 25%, el ataque le había producido pérdidas económicas. Solo el 16% tenía esta eventualidad cubierta por el seguro, mientras que el 84% no tenía el ataque cubierto.

No se trata únicamente de un riesgo para el sector marítimo: el pasado mes de junio, el sistema sanitario de Singapur fue objeto de lo que su gobierno calificó como *«un ataque cibernético deliberado, selectivo y bien planificado»*. Este sistema no contaba con un procedimiento de protección eficaz ni un plan de contingencia y se produjeron daños y pérdidas de información importantes. Un mes después, las autoridades tomaron la decisión de desconectar de internet todos los ordenadores de su sistema sanitario para así evitar que se puedan producir nuevos ataques y robos de información.

Todos los informes de expertos apuntan a que, mientras es muy difícil eliminar por completo el riesgo de ser objeto de un ciberataque, por el contrario, las tareas de definir y poner en práctica un plan básico de prevención y respuesta, complementado con un programa de formación del personal, pueden reducir muy notablemente las consecuencias en caso de ataque y ello con medidas realmente abordables en un plazo y a un coste asequibles, incluso en el caso de que sea necesario un asesoramiento técnico externo.

Definir y poner en práctica un plan básico de prevención y respuesta, complementado con un programa de formación del personal, pueden reducir notablemente las consecuencias de un ciberataque

BIMCO comenzó sus trabajos en este campo en 2016, publicando unas Pautas sobre ciberseguridad para las empresas marítimas, que revisó posteriormente y que desde ANAVE difundimos en el Cuaderno Profesional Marítimo de nuestro boletín mensual en septiembre de 2017. Cualquier empresa marítima, siguiendo dichas pautas, puede diseñar y poner en práctica planes eficaces: prevenir siempre es mejor que curar.

ANAVE
Asociación de Navieros Españoles
Dr. Fleming, 11 - 1ºD - 28036 Madrid - España.
Tel.: +34 91 458 00 40
anave@anave.es
www.anave.es