Buques ciber-resilientes, ¿Cómo proteger a nuestra flota de ciber-ataques?

OSCAR NAVARRO - DIRECTOR DE CIBERSEGURIDAD INDUSTRIAL S2 GROUP
JUAN A. MOJÓN - DIRECTOR DIVISIÓN DE SOFTWARE Y NUEVAS TECNOLOGÍAS EN AEROMARINE

Actualmente nos encontramos ante un escenario de alto riesgo. El aumento en la conectividad entre sistemas, personas e incluso equipamiento industrial está aumentando el perímetro de defensa e incrementando la posibilidad de sufrir un incidente de ciberseguridad.

La Resolución MSC.428 (98) de la OMI persigue que todas las navieras desarrollen al menos un plan de ciberseguridad y de respuesta frente a ciberamenazas, como parte del Manual de Gestión de la Seguridad de cada buque, a más tardar en la primera verificación anual del Documento de Cumplimiento de la compañía después del 1 de enero de 2021. Las exigencias normativas y la adecuada valoración del riesgo existente y el posible impacto sobre el negocio son dos líneas que confluyen para impulsar al sector a tomar medidas.

En este artículo resumimos el contexto actual y analizamos las opciones que las empresas navieras tienen a su disposición a la hora de afrontar la ciberseguridad, comentando las iniciativas que se pueden implantar y algunos factores fundamentales para garantizar el éxito de las inversiones en ciberseguridad.

CONTEXTO

Durante el año 2020, los ciberataques han aumentado notablemente en la industria marítima. Atrás queda ya el tiempo en el que se pensaba que un buque era una isla protegida de influencias externas que pudieran condicionar la operación y el correcto funcionamiento de los sistemas IT/ OT instalados a bordo.

Durante los últimos 4 años hemos visto como algunas de las navieras más grandes como MAERSK, COSCO o CMA CGM eran atacadas, produciendo, en algunos casos, pérdidas millonarias que, sin duda, hubieran llevado a la quiebra a empresas más pequeñas del sector.

Pero las navieras no han sido las únicas en sufrir este tipo de ciberdelincuencia, instalaciones portuarias, e incluso los servidores de la Organización Marítima Internacional (OMI) han tenido que lidiar con ciberataques de distinta índole.

¿CUÁLES SON LAS CAUSAS DEL INCREMENTO DE LOS CIBERATAQUES?

Las razones principales del aumento de los ciberataques son la evolución tecnológica y la digitalización de los procesos de a bordo.

Hoy en día se han abaratado las comunicaciones buque / tierra, lo que permite a las empresas adoptar sistemas de gestión avanzados, poner en marcha proyectos basados en big data, obtener datos de los sistemas IT /OT desde tierra e incluso efectuar labores de mantenimiento en remoto.

A esto debemos sumar los cambios evolutivos de los sistemas más importantes del buque, como los de navegación o propulsión, que permiten el intercambio de información a través de redes TCP/IP, la configuración y control a través de aplicaciones de software o el seguimiento de su operación desde consolas externas dentro y fuera del buque.

LA RESOLUCIÓN MSC.428(98) DE LA OMI

El aumento de los ciberataques ha despertado a una parte sector. Muchas navieras llevan tiempo aplicando guías de buenas prácticas, creando y mejorando procedimientos de seguridad de la información y concienciando a sus tripulantes sobre las amenazas, los riesgos y la co-

rrecta utilización de los equipos IT y OT de los buques.

La OMI, por su parte, consciente de la nueva realidad del sector, ha adoptado la Resolución MSC.428 (98) que persigue que todas las navieras desarrollen al menos un plan de ciberseguridad y de respuesta frente a ciberamenazas, como parte del Manual de Gestión de la Seguridad (Código ISM) de cada buque.

La normativa ha entrado en vigor el 1 de enero de este año, y obliga a las empresas a auditar este nuevo plan de seguridad, a más tardar, en la primera verificación anual del Documento de Cumplimiento de la compañía después del 1 de enero de 2021.

PERO ¿ES ESTO SUFICIENTE PARA QUE LOS BUQUES SEAN RESILIENTES?

Lamentablemente la respuesta es no. Seguir la recomendación de la OMI, como hemos mencionado anteriormente, nos permitirá establecer los procedimientos necesarios para conocer los activos que tenemos que proteger, cuáles son sus vulnerabilidades y las amenazas a las que están expuestos, e instruir a los tripulantes sobre cómo proceder en cada caso, propiciando de esta manera una cultura de ciberseguridad en la flota.

Si lo que queremos es proteger nuestro negocio, deberemos implantar una serie de medidas de seguridad que se definirán después de un análisis exhaustivo de cada instalación.

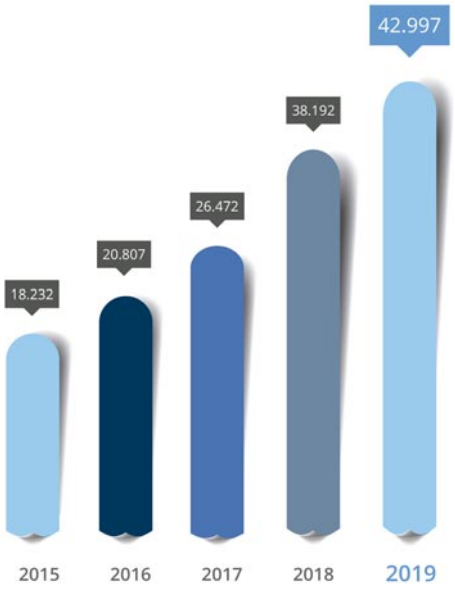
IMPLANTANDO MEDIDAS DE SEGURIDAD EN LOS BUQUES

Uno de los primeros aspectos que se debe tener en cuenta a la hora de trabajar en la seguridad de un buque o una flota es que la seguridad es un proceso y que, por tanto, constituye una tarea que debe incorporarse a las actividades propias de cada compañía, para garantizar su continuidad en el tiempo.

No existe ningún sistema del que pueda decirse que es completamente seguro o que no pueda tener vulnerabilidades no conocidas. Por otra parte, la tecnología y la forma en la que se utiliza cambia. Por esta razón, lo primero es adaptar la organización a esta nueva realidad: la ciberseguridad no es algo que se compra una vez y se tiene, sino un proceso continuo.

A partir de aquí, la primera línea de trabajo debe ser necesariamente llevar a cabo un análisis que permita obtener una imagen del estado de protección del buque.

Para ello es preciso aunar conocimientos especializados del sector marítimo con los conocimientos específicos de ciberseguridad: un buque es un sistema complejo que depende para su operación de multitud de subsistemas, algunos típicamente industriales (generación de energía, propulsión, sistemas eléctricos, antiincendios, etc.) y otros específicos como la navegación, la gestión del pasaje o carga, etc.



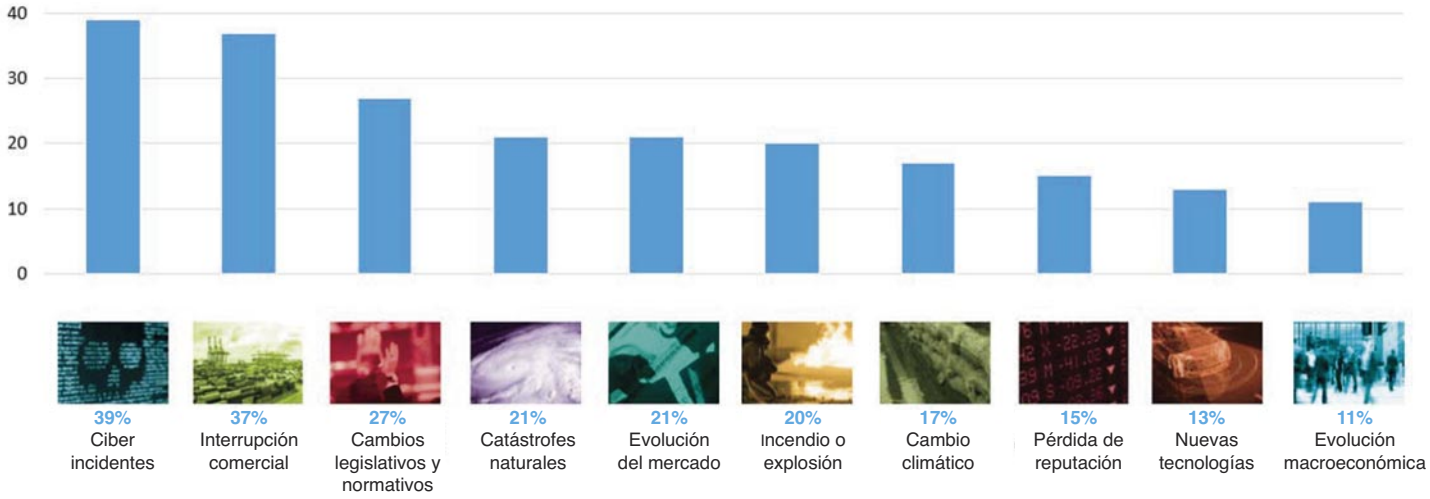
Incidentes relacionados con la ciberseguridad. Fuente: Centro Criptológico Nacional, CCN-CERT.

El objetivo es identificar situaciones de riesgo que, de materializarse, podrían afectar a los procesos de negocio que dependen del buque, a la seguridad de las personas, el medio ambiente y los bienes materiales (el propio buque y su carga).

La gran heterogeneidad del sector marítimo hace recomendable que estos análisis se efectúen de forma individualizada, requiriendo incluso la realización de pruebas de carácter técnico a bordo. En este tipo de análisis se identifican, típicamente, debilidades asociadas al acceso físico a los equipos o sistemas, errores de configuración, de gestión de accesos, arquitecturas deficientes o prácticas de mantenimiento u operación inseguras (incluyendo el trabajo de empleados propios o terceros externos), gestión deficiente de conexiones remotas o accesos locales, etc.

Estos análisis técnicos, incluyan o no un test de intrusión, deben llevarse a cabo con las adecuadas garantías para no causar daños en los sistemas evaluados. Debe conseguirse un equilibrio entre la necesidad de realizar hacer y los riesgos implicados en su ejecución. Un buen plan de pruebas es fundamental para garantizar este equilibrio.

Sin embargo, la adopción de medidas a posteriori siempre dificulta su aplicación y limita su eficacia, por lo que lo ideal es integrar la ciberseguridad en el ciclo de vida completo del buque, comenzando por la definición de especificaciones de ciberseguridad de aplicación durante el proyecto, la construcción, la com-



Principales riesgos a los que se enfrenta la industria internacional. Fuente: Allianz Risk Barometer 2020

pra de equipos, la contratación de servicios, etc.

A posteriori, en la fase de proyecto y construcción, hay que garantizar que las especificaciones de ciberseguridad definidas son efectivamente implantadas, pudiendo incorporarse análisis específicos como parte de las pruebas del buque.

Otro elemento fundamental es la monitorización de actividad anómala tanto en el uso de los equipos de a bordo como en las redes de comunicaciones internas y externas. El diseño, despliegue y operación de estos sistemas de monitorización de la ciberseguridad en buques tienen aspectos comunes con otros sectores.

Aun así, deben adaptarse a los aspectos específicos de este entorno a la hora de afrontar asuntos como:

- La elección de los sistemas a monitorizar: perímetros, redes, equipos, etc.
- La posibilidad de instalar equipamiento de ciberseguridad a bordo, teniendo en cuenta limitaciones de espacio, electrónica de red, etc. No es raro tener que hacer modificaciones en la infraestructura para permitir estos despliegues.
- La definición de un conjunto acotado de situaciones de riesgo potencial, específicas, que tengan sentido en el contexto concreto del buque monitorizado.
- El modelo elegido para la atención de las alertas de ciberseguridad en función de las opciones de comunicación: online, en tiempo real u *offline*, cuando la conectividad lo permita.
- La propia definición de las alertas, que debe permitir la toma de decisiones por parte de la tripulación. Hay que tener en cuenta que este personal no tiene, por lo general, conocimientos avanzados de ciberseguridad y por lo tanto la caracterización de la amenaza y el posible impacto deben definirse claramente. Lo mismo se aplica a la comunicación con el personal que pueda apoyar desde tierra y que, necesariamente, tendrá que comunicarse con la tripulación.

Este tipo de aproximación basada en el conocimiento específico de los sistemas que se quieren proteger permite garantizar el éxito de las inversiones, evitando situaciones que se están produciendo en otros sectores: cada vez es más habitual encontrar casos en los que un planteamiento basado en el despliegue de equipamiento estándar no alcanza los objetivos deseados.

En este sentido, la puesta en marcha de proyectos piloto permite adquirir experiencia en el proceso, poner a prueba la tecnología y obtener información para el diseño de procesos de despliegue de tecnologías de monitorización a una escala mayor.

Por último, y en línea con lo indicado más arriba, **es imprescindible integrar las evaluaciones periódicas de ciberseguridad en los procesos de auditoría** para garantizar que los controles implantados, tanto técnicos como procedimentales, son operativos, adecuados a las amenazas existentes y se aplican correctamente.

EL COSTE DE LA NO-SEGURIDAD

El proceso de análisis e implementación de medidas descrito anteriormente tiene un coste, debe incluir toda la estructura IT / OT de cada buque, y ser revisado constantemente para que sea efectivo, reduzca el riesgo de ataque a lo largo de toda la vida operativa del buque y minimice las consecuencias en caso de producirse.

No obstante, para analizar la rentabilidad o no de tener una flota resiliente, debemos estudiar cuáles son las consecuencias económicas para nuestro negocio en caso de que se produzca un ataque que afecte a nuestra actividad.

Actualmente nos encontramos ante un escenario de alto riesgo. El incremento en la conectividad entre sistemas, personas e incluso equipamiento industrial está acrecentando el perímetro de defensa, aumentando la posibilidad de sufrir un incidente de ciberseguridad. Además, la creciente interrelación entre sectores, negocios y cadenas de valor hacen que eventos que a priori tienen un impacto limitado, puedan propagarse y acabar impactando sobre las operaciones de una gran compañía.

Esta situación se refleja perfectamente en las cifras de incidentes gestionados por el Centro Criptológico Nacional, CCN-CERT. Según se recoge en su In-

forme Anual de Amenazas y Tendencias 2020(1), en 2019, el CCN-CERT gestionó 42.997 ciberincidentes, con un aumento superior al 11 % con respecto al año anterior, de los cuales casi un 7,5 % fueron de peligrosidad muy alta o crítica.

El sector empresarial percibe el riesgo creciente asociado a los ciberincidentes, que ha crecido en los últimos años hasta convertirse en la principal preocupación. Así lo identifica Allianz en su Informe Anual(2) sobre los principales riesgos a los que se enfrenta la industria internacional, que sitúa los problemas derivados de ciberincidentes como el principal riesgo a gestionar.

En lo relacionado específicamente con el sector marítimo, todo el mundo recuerda el ciberataque sufrido en 2017 por la naviera Maersk, que obligo a la empresa a paralizar sus operaciones durante semanas y que tuvo un coste económico de entre 250 y 300 millones de dólares.

Pero este incidente no es un caso aislado. En 2018, la naviera COSCO sufrió un ataque que afectó a sus operaciones en Estados Unidos; en abril de 2020, la naviera MSC vio comprometida su sede de Ginebra; en septiembre de 2020 CMA CGM anunció que un ciberataque había afectado a sus servidores periféricos; e incluso la infraestructura IT de OMI ha sido objeto de un ataque informático el pasado año.

Los casos de ciberataques crecieron exponencialmente en 2020 en el sector y, aunque la mayoría de ellos no eran dirigidos, es decir, eran ataques lanzados para 'pescar' a cualquier empresa, también se han detectado ataques dirigidos, que tienen como fin deteriorar la imagen, robar información confidencial o causar daño a una empresa concreta.

Para evaluar si la implantación de medidas de ciberseguridad en una naviera será rentable, tendríamos que contestar a preguntas como:

- ¿A cuánto ascendería la pérdida económica en el caso que se produzca un robo de información confidencial de la empresa?
- ¿Qué pierde mi empresa por cada día de inoperatividad total de uno de mis buques? ¿Y de toda la flota?
- ¿Cuáles son los riesgos personales a los que se enfrentan las tripulaciones en el caso de que un ciberataque de lugar a un accidente en uno de mis buques?
- ¿Cómo afectaría la perdida de sistemas IT como software de carga y descarga, plataformas de reservas, sistemas de control de viajes o ERPs en el día a día de la compañía?
- ¿En el caso de que suframos un ataque, cual es la inversión necesaria para volver a la normalidad?

En nuestra opinión, las medidas de la seguridad de la información de cada uno de los centros de trabajo de una empresa deben formar parte del plan estratégico, de forma que se analice qué procedimientos deben de modificarse y qué medidas se han de adoptar a corto, medio y largo plazo para garantizar la estabilidad y la rentabilidad de la actividad. Por otra parte, no se debe olvidar que, en este contexto de alto riesgo, la ciberseguridad puede convertirse en un factor competitivo fundamental que puede decidir qué compañías sobreviven y cuáles no.

CONCLUSIONES

En definitiva, nos encontramos ante un nuevo escenario en el que el riesgo creciente de sufrir un ciberataque y su impacto potencial en el negocio no puede ser ignorado. Tanto la realidad constatada en los ataques sufridos por empresas navieras y otros organismos del sector, como los avances normativos comentados anteriormente, fijan el horizonte para todos los participantes del sector.

Las medidas a nuestro alcance son de distinta índole, y van desde la adopción de soluciones tecnológicas hasta el aumento de las habilidades de las tripulaciones.

En cualquier caso, la ciberseguridad debe afrontarse como un elemento más de las operaciones, integrándola en los procesos de negocio e implementando los cambios organizativos necesarios para garantizar la rentabilidad de las inversiones y su efectividad en el tiempo.

Por último, el coste de la ciberseguridad debe evaluarse contra el impacto económico potencial de un solo incidente, realizando los análisis de riesgos necesarios que permitan poner en contexto estas inversiones y comparándolas con **el coste de la no-seguridad.**

CIBERATAQUE A.P. MOLLER MAERKS (2017)

1. **Mecanismo:** ataque a la cadena de suministro. El malware (Not Petya) se introdujo en los sistemas de la compañía por medio de un software de gestión suministrado por un proveedor especializado.
2. El **ataque** afectó a los sistemas de sus terminales portuarias en todo el mundo.
3. Se produjo un **impacto** generalizado en los sistemas. Todas las actividades de sus terminales quedaron paralizadas.
4. El **impacto económico** se estimó entre 250 y 300millones de dólares.
5. **Acciones de recuperación:** Volver a instalar todos los servidores y estaciones de trabajo de la compañía: unos 40.000 ordenadores y 4.000 servidores.

(1) El informe completo Amenazas y Tendencias 2020 del Centro Criptológico Nacional puede descargarse en este enlace.

(2) El Informe Anual de Allianz puede descargarse en este enlace.