Maritime Cyber Security Stats and Facts – Spanish

HECHOS

Escenarios en los que pueden producirse lesiones debido a ciber incidentes marítimos

1. El sistema de navegación de un buque se ve comprometido a través de un ciberataque y da lugar a datos de navegación incorrectos o manipulados que provocan colisiones con otros buques, varadas o incidentes que afectan a infraestructuras marítimas como puentes o estructuras en alta mar.
2. Los ciberataques dirigidos a los sistemas de motor o maquinaria de un buque pueden causar fallos en el motor, mal funcionamiento del sistema de propulsión o pérdida de potencia, lo que puede provocar accidentes y lesiones.
3. Los incidentes cibernéticos que interrumpen los sistemas de comunicación, incluidos los canales de comunicación de buque a buque, de buque a tierra o de emergencia, pueden obstaculizar la coordinación y la respuesta eficaces durante situaciones críticas.
4. Si los sistemas de seguridad de los buques marítimos, como la extinción de incendios, los sistemas de alarma y los mecanismos de respuesta de emergencia, se ven comprometidos a través de ciberataques, se deteriora su funcionalidad, lo que puede provocar retrasos o respuestas inadecuadas a los incidentes de seguridad y aumentar el riesgo de lesiones.
5. Los incidentes cibernéticos dirigidos contra los sistemas de control de acceso, como cerraduras electrónicas, cámaras de seguridad o mecanismos de control de entrada, dan lugar a un acceso no autorizado a zonas sensibles de un buque o instalación marítima.

ESTADÍSTICAS

- Tres cuartas partes de los profesionales marítimos creen probable que un incidente cibernético obligue a cerrar una vía navegable estratégica (76%). Más de la mitad espera que los ciberataques provoquen colisiones de buques (60%), encallamientos (68%) e incluso provoquen lesiones físicas o la muerte (56%), ya que una abrumadora mayoría (79%) de los profesionales afirma que el sector considera que los riesgos de ciberseguridad son tan importantes como los riesgos para la salud y la seguridad.
    - Según la encuesta, apenas 3 de cada 10 (31%) profesionales marítimos creen que las organizaciones de su sector son eficaces a la hora de compartir información y lecciones aprendidas sobre riesgos, amenazas e incidentes de ciberseguridad.
- En el frente de la ciberseguridad, 2021 no fue un buen año para la industria marítima y logística. La frecuencia de los ataques contra buques aumentó un 33%, tras un aumento del 900% de los ataques contra buques y sistemas portuarios en 2020.
- En una encuesta sobre ciberseguridad marítima realizada por Safety at Sea y BIMCO en 2020, a pesar de que la mayoría de los encuestados (77%) considera los ciberataques como un riesgo alto o medio para sus organizaciones, pocos parecen estar preparados para las consecuencias de un ataque de este tipo. El 64% de los encuestados afirmaron que su organización dispone de un plan de continuidad de la actividad que debe seguirse en caso de incidente cibernético, pero sólo el 24% afirmó que se ponía a prueba cada tres meses, y sólo el 15% afirmó que se ponía a prueba cada seis a doce meses. Sólo el 42% de los encuestados afirma que su organización protege los buques de las ciberamenazas de la tecnología operativa (OT).