RESUMEN

Este estudio, desarrolla una metodología para analizar y evaluar los ciberriesgos de un buque civil. Proponemos un plan de contingencia, medidas de defensa y de recuperación de los sistemas involucrados en un incidente de ciberseguridad. La amenaza al sector marítimo no es ficción, ya existen diversos incidentes y las consecuencias de un ataque podrían ser catastróficas. En los últimos años, se han multiplicado los episodios de ataques a equipos, redes a nivel mundial y la ciberseguridad es de la máxima importancia para los estados, los cuales publican y actualizan leyes para intentar frenar estas actividades que tanto perjudican a todos los sectores.

Debemos de proveernos de las mejores soluciones tecnológicas de seguridad que tengamos al alcance y realizar una monitorización continua, lo que nos dará a conocer en todo momento, qué protecciones tenemos y cuáles son los riesgos potenciales a los que nos enfrentamos. El incremento, ya imparable, del uso de la tecnología en la nube para controlar los sistemas de a bordo, tanto desde el propio buque como desde tierra por la compañía naviera, añade un escenario complejo que agrava la situación de defensa frente a posibles amenazas.

Las empresas marítimas, han de tener sistemas informáticos rígidos aplicando múltiples capas de medidas de protección y han de establecer un riguroso control de los usuarios y de los permisos de acceso a los sistemas.

PALABRAS CLAVE

Seguridad Marítima, Ciberseguridad Marítima, DAFO, Terrorismo Marítimo, Hackers, Malware, Sistema de Seguridad Nacional, Plan de Contingencia.

ABSTRACT

This academic study develops a methodology to analyze and evaluate the cyber risks of a motor merchant. We propose a contingency plan, defense measures and recovery of the systems involved in a cybersecurity incident. The threat to the maritime sector is not fiction, there are already several incidents and the consequences of an attack could be catastrophic. In recent years, episodes of attacks on computers and networks have multiplied worldwide and cybersecurity is of the utmost importance for states, which publish and update laws to try to stop these activities that are so damaging to all sectors.

We must provide ourselves with the best technological security solutions available to us and carry out continuous monitoring, which will let us know at all times what protections we have and what are the potential risks we face. The already unstoppable increase in the use of cloud technology to control on-board systems, both from the ship itself and from the shore by the shipping company, adds a complex scenario that aggravates the defense situation against possible threats.

Maritime companies, must have rigid computer systems applying multiple layers of protection measures and must establish rigorous control of users and access permits to the systems.

KEYWORDS

Maritime Safety, Maritime Cibersecurity, DAFO, Terrorism, Hackers, Malware, National Security System, Contingency Plan.