Shipping Italy

Il quotidiano online del trasporto marittimo

Perché l’addestramento del personale è la prima linea di difesa contro gli attacchi informatici

Nicola Capuzzo · Monday, December 29th, 2025

*Contributo a cura di Sandro Stefani**

** Marine Digital Consultancy Services & Training*

Il settore marittimo è sempre più digitalizzato: dai sistemi di navigazione alle piattaforme di gestione operativa, ogni componente è connesso. Questa evoluzione porta efficienza, ma anche nuove vulnerabilità. Il recente attacco cyber al traghetto *Fantastic* di GNV ha riportato in primo piano un tema cruciale: la sicurezza informatica in ambito navale. Non si tratta solo di tecnologia, ma di persone e organizzazioni. Il fattore umano è il vero punto debole e la formazione è lo strumento chiave per trasformarlo in punto di forza.

Negli ultimi anni l’IMO ha integrato la gestione del rischio cyber nell’ISM Code, mentre IACS ha introdotto requisiti obbligatori per la cyber-resilienza nelle nuove costruzioni. Linee guida di BIMCO, INTERTANKO e OCIMF insistono sulla formazione del personale di bordo a tutti i livelli. Ma cosa deve includere un programma efficace? Quattro pilastri: **consapevolezza**, **gestione tecnica**, **procedure e responsabilità**, **esercitazioni pratiche**. I corsi possono essere in aula o online, con durate che vanno da poche ore introduttive a moduli avanzati con simulazioni.

Tra le metodologie emergenti spicca l’approccio **role-based**, che adatta i contenuti alle funzioni operative. Il progetto MarCy, sviluppato da accademia e industria, segue questa logica e punta a ridurre l’errore umano attraverso moduli personalizzati e scenari realistici. L’obiettivo è creare una vera “cultura della consapevolezza”, non interventi spot.

Perché è così importante? Gli attacchi cyber non mirano a “prendere il controllo” della nave – ipotesi remota – ma a penetrare nella rete IT e sottrarre dati sensibili su passeggeri e carichi. Un attacco ransomware può bloccare le operazioni portuali per giorni, con costi che superano milioni di euro. In un contesto di guerra ibrida, il rischio è concreto e le conseguenze possono essere gravi. Eppure, secondo analisi di DNV, Thetius e CyberOwl, il 31% delle compagnie ha subito un attacco, il 71% del management è consapevole del problema, ma il **93% del personale di bordo non ha ricevuto formazione specifica**.

Serve un cambio di paradigma: **formazione continua**, certificazioni, moduli per ruolo, simulazioni realistiche e aggiornamenti periodici. Non si tratta solo di rispettare le normative, ma di investire in resilienza digitale come vantaggio competitivo. Gli attacchi informatici sono come l'Idra di Lerna: ogni testa recisa ne genera altre. L'unica arma efficace è la conoscenza, distribuita e aggiornata lungo tutta la vita professionale. Gli armatori che comprendono questo principio non solo riducono il rischio, ma garantiscono continuità operativa e fiducia dei clienti in un mercato sempre più interconnesso.

This entry was posted on Monday, December 29th, 2025 at 7:45 am and is filed under Economia
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.