PERIODICO MARITTIMO INDIPENDENTE A DIFFUSIONE INTERNAZIONALE
A BILINGUAL SHIPPING NEWSPAPER
L'INFORMATORE NAVALE
FONDATO NEL 1964 di NAPOLI

Cybersecurity e digitale al centro del workshop organizzato da RINA e Confitarma

Nella splendida cornice di Palazzo Colonna a Roma si è tenuto il workshop "Cybersecurity e digitale: evoluzione normativa e compliance per le società di navigazione", organizzato da RINA in collaborazione con Confitarma

L'evento ha visto la partecipazione di ***Nicolò Rivetti di Val Cervo****, Capo Divisione NIS del Servizio Regolazione ACN (Agenzia per la Cybersicurezza Nazionale);* ***Luca Carrà****, Marine Automation & Cyber Security Product Manager di RINA e* ***Mario Caligiuri****, Presidente di SOCINT e docente dell'Università della Calabria*

Durante i lavori, sono state analizzate le complesse e rapide sfide legate alla cybersecurity nel settore marittimo. Gli interventi si sono concentrati sui recenti sviluppi normativi, con particolare attenzione alla valutazione del rischio, all'adozione di misure tecniche e organizzative efficaci, e all'implementazione di best practice per la sicurezza informatica "a bordo".

L'incontro ha evidenziato la necessità di una stretta collaborazione tra tutti gli attori del settore per costruire un sistema digitale resiliente e preparato ad affrontare le sfide future.

Ad aprire i lavori **Cesare d'Amico**, Vice Presidente e Presidente del GDL Cyber/Maritime Security di Confitarma, che ha sottolineato come *"la sicurezza della navigazione sia fondamentale per la competitività dell'industria dei trasporti marittimi e del Paese. In ambito di safety e security, la gestione delle minacce cibernetiche rappresenta una priorità per lo shipping. Questo richiede un approccio puntuale e approfondito."*

"In considerazione della crescente rilevanza della cybersecurity - ha aggiunto il Direttore Generale di Confitarma **Luca Sisto** - *auspichiamo l'introduzione di interventi legislativi mirati che destinino fondi pubblici, anche attraverso il PNRR per la digitalizzazione, per supportare la formazione del personale delle imprese di navigazione, sia a bordo sia a terra."*

"La cybersecurity rappresenta una sfida cruciale per il settore marittimo, che richiede un continuo aggiornamento per affrontare i rischi cibernetici derivanti dall'introduzione nei nuovi design nave di soluzioni tecnologiche innovative integrate - ha aggiunto **Luca Carrà**, Marine Automation & Cyber Security Product Manager di

RINA -. *Inoltre, è fondamentale rimanere allineati con un panorama normativo in costante evoluzione. Eventi come questo workshop non solo offrono un'importante occasione di confronto tra esperti e operatori del settore ma aiutano anche le compagnie di navigazione a comprendere meglio le implicazioni della Direttiva NIS2, a familiarizzare con i nuovi requisiti IACS UR E26 ed E27, applicabili alle nuove costruzioni contrattualizzate dal 1° luglio 2024, preparandosi quindi a gestire i rischi in modo efficace. Questo approccio è essenziale per garantire un futuro digitale più resiliente e sicuro."*

Il workshop ha affrontato anche i cambiamenti normativi in atto sottolineando la necessità di un adeguamento puntuale per le compagnie di navigazione.

Da ottobre 2024 è in vigore la Direttiva NIS2, che include le compagnie di navigazione definite come medie imprese a livello europeo. Entro aprile 2025, l'Italia dovrà definire un elenco di soggetti essenziali e importanti, eventualmente comprendendo anche piccole e medie imprese. Nel corso della mattinata si è parlato anche dell'introduzione dei nuovi requisiti IACS UR E26 (Cyber Resilience of Ships – Requirements for Ship Owners/Operators) ed E27 (Cyber Resilience of Ships – Requirements for Equipment Suppliers), specificatamente dedicati alla sicurezza cibernetica, obbligatori per le nuove costruzioni contrattualizzate dal 1° luglio 2024. I design delle nuove navi che andranno ad ampliare le flotte esistenti dovranno quindi incorporare questi requisiti fin dalla fase progettuale.

Gli armatori, consapevoli dell'importanza del tema, hanno già investito in infrastrutture IT sicure e implementato procedure specifiche per integrare i rischi informatici nei propri Safety Management System, in conformità al Codice Internazionale di Gestione della Sicurezza (ISM Code) dell'IMO.

Le compagnie di navigazione sono chiamate a prepararsi al recepimento del Cyber Resilience Test Procedure, essenziale per garantire una corretta postura cyber delle nuove unità. Questo approccio proattivo non solo mitiga i rischi cibernetici derivanti da tecnologie avanzate e integrazioni complesse ma assicura anche la conformità con le normative emergenti, salvaguardando la resilienza digitale a bordo delle navi.