Shipping Italy
Il quotidiano online del trasporto marittimo

Red team e non solo: le armi della Difesa contro attacchi cyber alle navi (anche commerciali)

Nicola Capuzzo · Saturday, February 19th, 2022

Chi meglio della Marina Militare può offrire consigli su come contrastare un attacco alla propria flotta navale? Se l'offensiva è di tipo cyber, la prima difesa deve però essere disposta già nella fase di procurement delle stesse unità, ha evidenziato Gianluca Maria Marcilli, Capitano di Fregata della Direzione degli Armamenti Navali, nel corso di un webinar sul Cyber Risk organizzato dal Propeller di Milano.

Dopo una introduzione a cura di Alessio Franconi (Giovani Propeller Milano) e un intervento dedicato al tema della sicurezza informatica nelle aziende di Michele Perugini (Giovani Propeller Napoli), la presentazione di Marcilli è stata dedicata specificamente alle linee guida in materia di cybersecurity osservate dalla Navarm (appunto, la Direzione degli Armamenti Navali della Difesa) negli acquisti di naviglio.
Il Cf ha innanzitutto inquadrato il tema evidenziando la necessità di un orientamento alla security by design, ovvero che tenga in conto degli aspetti della sicurezza informatica già in fase di progettazione. Necessario predisporre un piano di valutazione dei rischi e la definizione delle azioni di mitigazione, con un approccio però che tenga conto del fatto che, a differenza di quanto avviene in altri ambiti, le minacce cyber sono in continua evoluzione e quindi le iniziative di contrasto dovranno essere continuamente aggiornate. Banalmente – ha invitato a riflettere Marcilli- una nave ha solitamente un ciclo di vita di 30 anni, mentre un sistema operativo standard (da Windows Xp in poi) dura al massimo poco più di decina d'anni. La sua obsolescenza non dovrà diventare un fattore di rischio per il mezzo. Fondamentale poi, secondo il Capitano di Fregata, inserire i requisiti di sicurezza cyber all'interno dei contratti: nel caso di una unità commerciale (a differenza ad esempio di quanto può valere per un sommergibile) si potrà valutare quali rischi potranno essere considerati accettabili in modo da bilanciare necessità di security e costi. Un aiuto in questo senso può essere tratto dagli standard ISO/IEC 27001 e ISO/IEC 27002, norme internazionali che contengono i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni e che possono essere utilizzate come riferimento dalle divisioni It delle aziende coinvolte.

L'ultimo consiglio di Marcilli (quello che più sembra evocare uno scenario da guerra) agli armatori di navi mercantili è infine di creare un Red team. In altre parole, dare vita a una "squadra d'assalto" che, in contraddittorio con la design authority, simuli o metta realmente in atto (in un contesto protetto) attacchi senza esclusione di colpi ai sistemi informatici della nave per scovarne

tutte le eventuali debolezze.

F.M.

ISCRIVITI ALLA NEWSLETTER QUOTIDIANA GRATUITA DI SHIPPING ITALY

This entry was posted on Saturday, February 19th, 2022 at 11:00 am and is filed under Navi
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.