Shipping Italy

Il quotidiano online del trasporto marittimo

Settore marittimo e cybersicurezza: crescono gli attacchi, e insieme, i pericoli

Nicola Capuzzo · Wednesday, November 1st, 2023

Questo contenuto rientra fra quelli pubblicati all'interno dell'inserto ***Rischi e assicurazioni nei trasporti – edizione 2023***

*Contributo a cura di Alessio Aceti **

** amministratore delegato Hwg Sababa*

L'odierno settore marittimo si affida sempre più alla digitalizzazione, all'integrazione operativa e all'automazione, con i principali costruttori e operatori navali che investono nell'innovazione utilizzando tecnologie e sistemi all'avanguardia per creare navi con capacità avanzate di controllo remoto, comunicazione e connettività. Una digitalizzazione che si estende anche alle strumentazioni portuali, che sono sempre più avanzate, ma soprattutto connesse.

Finora questo settore era considerato sicuro a causa della mancanza di connettività Internet e della natura isolata delle navi in mare, ma, secondo il report "Cybersecurity Challenges in the Maritime Sector", sta registrando un aumento del 900% delle violazioni di cybersicurezza sulla tecnologia operativa.

Le navi, tra le infrastrutture che utilizzano servizi digitali, sono fra le più critiche poiché l'interruzione dolosa delle loro operazioni può portare a danni finanziari, ambientali o addirittura mettere in pericolo la sicurezza delle persone. Sebbene siano state condotte alcune ricerche in questo settore, la cybersicurezza marittima non è stata ancora studiata a fondo.

I sistemi automatizzati complessi integrati nelle navi moderne e autonome hanno reso il mare un luogo molto più sicuro rispetto al passato. Tuttavia, alcuni di questi sistemi sono spesso insicuri e vulnerabili dal punto di vista informatico perché considerati meno critici per la sicurezza e le prestazioni, offrendo nuove opportunità agli hacker e agli attori malevoli. Di fatto, negli ultimi anni sono stati molti gli attacchi che hanno avuto successo.

Le principali motivazioni di questi attacchi sono l'acquisizione del controllo remoto di navi e imbarcazioni, il furto di informazioni importanti e riservate che possono essere utilizzate per sferrare ulteriori attacchi, o l'interruzione delle operazioni navali mettendo fuori uso componenti importanti e rendendo indisponibili i sistemi automatizzati. Negli anni, diversi attacchi hanno portato alla collisione tra imbarcazioni, alla deviazione del loro percorso, all'alterazione della posizione GPS della nave che diventava così irrintracciabile, o addirittura alla compromissione dell'intero sistema di gestione della nave, fino ad arrivare a compromettere quello dell'intero porto.

I numerosi incidenti informatici riportati e le loro conseguenze dimostrano chiaramente che ogni nave, imbarcazione, o porto, è a rischio di attacchi informatici se i sistemi informativi chiave non sono adeguatamente protetti.

Per questo motivo è necessario che ci sia un grande investimento da parte di ogni attore coinvolto, un investimento che non è inizialmente tecnologico, ma di governance, procedure e processi. È necessario che ci siano procedure di cybersecurity stabilite e ben conosciute da tutti, procedure di incident response, regole chiare per i fornitori in ambito cyber e sistemi che siano ben configurati e aggiornati.

La prima cosa da fare è una gap analysis, misurando così l'adeguatezza della propria infrastruttura rispetto ai requisiti previsti dagli standard di riferimento. Da qui si definiscono una serie di interventi da mettere in atto ed è solo in questo momento che entrano in gioco le tecnologie.

Da un punto di vista pratico l'integrazione tecnologica sulle navi si scontra con un problema molto specifico: lo spazio, un bene molto prezioso che pone sfide considerevoli in termini di collocazione delle infrastrutture, in navi di tutte le dimensioni. Pensando ad esempio alle navi da crociera, ci troviamo di fronte a vere e proprie smart city galleggianti che combinano tecnologie all'avanguardia, comfort e rispetto dell'ambiente. Al centro di questo mondo in movimento si trovano dei Data Center, cuori digitali della nave. I sistemi IoT, la registrazione dei passeggeri, la gestione delle cabine, le telecamere di sorveglianza e molto altro passano attraverso questo hub. Tecnologie ad alta efficienza e hardware più performanti, devono aver chiaro anche l'obiettivo di minimizzare l'ingombro fisico dell'infrastruttura del Data Center.

Infine, elemento fondamentale, sono i training accompagnati da vere e proprie simulazioni di attacchi, con il personale di bordo. L'obiettivo è quello di valutare il comportamento del personale, e non la resilienza dell'infrastruttura IT, di fronte a un attacco ransomware. Tutta l'organizzazione, a seconda del ruolo, deve essere consapevole dei rischi cyber e delle eventuali conseguenze di una disattenzione.

Solo portando a termine questo processo che include gap analysis, training e implementazione tecnologica, si può avere una struttura sicura, che, in caso di attacco, protegga personale, passeggeri, materiali trasportati e informazioni, minimizzando il rischio di ipotetiche catastrofi.

This entry was posted on Wednesday, November 1st, 2023 at 9:25 am and is filed under Inserti speciali
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.