Shipping Italy
Il quotidiano online del trasporto marittimo

Il #NextGenerationShipping suona la sveglia ai porti in tema di cybersecurity

Nicola Capuzzo · Monday, October 11th, 2021

“Gli hacker non sono ragazzi con il cappuccio, ma organizzazioni criminali transnazionali con enormi disponibilità finanziarie” tanto che “il cyber crime è stato definito dal World Economic Forum di Davos la terza economia del mondo”.

Basterebbero queste considerazioni ad allarmare ogni realtà aziendale o ente, eppure nel mondo portuale e marittimo l’attenzione a questi fenomeni è ancora insufficiente. A dirlo è stata Katia Redini, Corporate Sales Manager di CY4Gate – società quotata all’Aim che offre soluzioni in questo ambito a imprese e soggetti governativi, come forze armate o agenzie di sicurezza – durante il convegno #NextGenerationShipping organizzato nell’ambito del Port&Shipping Tech che si sta svolgendo in questi giorni a Genova.

Solo in Italia, secondo i dati citati dalla manager, i danni provocati dai cyber attack (di vario genere: perdite finanziarie, danni a impianti, fermi alle attività, furto di dati, danni reputazionali e spese legali) pesano per quasi 7 milioni di euro all’anno, mentre il costo delle sole violazioni di dati è di 3 milioni.

Non bisogna peraltro dimenticare che, oltre alla IT (Information Technology), spesso la vittima degli hacker è la OT (Operational Technology), ovvero l’insieme di device di controllo di processi industriali, e che quindi le violazioni possono avere come conseguenze anche lesioni, perdite di vite, danni agli impianti o all’ambiente.

Nonostante diversi casi anche recenti abbiano alzato l’attenzione sul fenomeno (tra gli altri quelli ai portali di Cma Cgm e di Msc), la consapevolezza in ambito marittimo sul tema come detto è però scarsa. In particolare i porti rischiano di essere soggetti vulnerabili non solo per le scarse risorse allocate alla prevenzione di questo fenomeno ma anche per la stessa complessità dell’eco-sistema portuale e la sua forte interconnessione con diversi attori.
I porti, in altre parole, già per loro natura permeabili, grazie alla presenza di diversi sistemi tecnologici (Pcs, Tos, Pmis e così via) sono accessibili a diversi soggetti ‘esterni’ all’organizzazione, e questo rappresenta un particolare elemento di rischio. “Gli attacchi spesso vengono fatti utilizzando i fornitori” ha riassunto Redini, ricordando che spesso è il fattore umano a determinare la riuscita di un attacco, motivo per cui gli hacker dedicano molte energie allo studio di tecniche di cosiddetto social engineering.

Le navi, in questo scenario, non sono però da meno come potenziali vittime di attacchi. Anche nel loro caso la presenza di reti IT e OT strettamente interconnesse (per la presenza di sistemi di controllo di potenza, gestione macchine e propulsione, comunicazione, servizi per la gestione del carico, dell'equipaggio o per i passeggeri) le rende un terreno fertile. Tra questi – ha esemplificato Redini – si possono citare aggressioni a reti Oem o a un fornitore di terze parte che si diffonde nella rete Ot della nave cliente, attacchi a provider di satelliti che così ottengono l'accesso alle reti It e Ot della unità oppure vulnerabilità per ottenere il controllo di sistemi Gps di navigazione, l'apertura o chiusura di valvole critiche o anche il controllo della zavorra.

F.M.

This entry was posted on Monday, October 11th, 2021 at 1:00 pm and is filed under Navi, Porti
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.