Shipping Italy
Il quotidiano online del trasporto marittimo

Italia al 4° posto per attacchi cyber; port authority nel mirino

Nicola Capuzzo · Monday, June 19th, 2023

“Nel 2022 si sono verificati 600 incidenti di Cybercrime contro i 400 del 2021 con una crescita del 50% anno su anno; il 24,21% ha interessato attacchi alla Pubblica Amministrazione, seguiti dai Servizi Pubblici generali per un 12,43% e dai Trasporti che ormai costituiscono il 4,32% degli incidenti. Le principali minacce per l’Italia sono Ransomware, Malware, Ingegneria Sociale, Furto di Dati, Threat against availability, Disinformation – Misinformation, Supply Chain Attacks. In particolare l’Italia è il 4° Paese per attacchi ransomware, dopo Stati Uniti, Germania e Francia”.

Questo il quadro emerso nel convegno tenutosi la scorsa settimana presso Confitarma, organizzato da “Esri Italia e WhereTech dal titolo cybersecurity e digitale: la sfida per i porti italiani” durante il quale si è discusso anche di un presunto “cyberattacco di tipo Ddos contro i siti web di 11 Autorità di Sistema Portuali Italiane” che sarebbe stato condotto dal “gruppo di hacker russi Noname 057”.

Il Convegno organizzato con il patrocinio di Espo (European Sea Ports Organisation), Assoporti, Confitarma e Federlogistica ha visto l’apertura Istituzionale del viceministro Edoardo Rixi per il Ministero delle Infrastrutture e Trasporti: “La riforma dei Porti Italiani e la forte spinta alla digitalizzazione nonché la condivisione dei dati attraverso la piattaforma logistica nazionale porta con sé un rischio altissimo di attacchi cibernetici. Non possiamo permetterci una interruzione della catena di gestione di una parte importantissima dell’industria italiana. Ben vengano contromisure sofisticate e condivise”.

A fargli eco il sottosegretario Matteo Perego di Cremnago per il Ministero delle Difesa: “Più aumenta l’intelligenza del porto, più aumenta il rischio, attaccare un porto significa attaccare la catena di approvvigionamento del Paese, più aumentano le tensioni geopolitiche e più siamo vulnerabili. Dobbiamo andare verso una struttura dove l’attacco ad un singolo scateni una reazione di sistema sinergica, efficace e con più potenza di fuoco”.

Il convegno è proseguito con l’intervento dell’Ammiraglio Andrea Billet dell’Agenzia Nazionale per la Cybersecurity e con la relazione di Gianfranco Elena della Nato: “Le interconnessioni tra infrastrutture possono essere di tipo fisico, ambientale, cibernetico e sono tra loro dipendenti, a tal punto che il grado di interconnessione ha un effetto reciproco sulle funzioni operative. Nel campo della sicurezza delle Infrastrutture Critiche attori pubblici e privati si trovano a cooperare proprio in ragione dell’interconnessione delle infrastrutture stesse, che diventano così realtà più complesse e reciprocamente dipendenti, e che necessitano di coordinamento per affrontare le vulnerabilità che

in tale sistema reticolare potrebbero portare ad un pericoloso effetto domino”.

Secondo gli organizzatori di Esri Italia, in conclusione, “con lo sviluppo delle piattaforme digitali, OT e IoT, le nostre infrastrutture critiche come i porti italiani hanno la necessità di avere un Digital Twin per monitorare continuamente la vulnerabilità. Le minacce alla sicurezza informatica diventano sempre più complesse: si propagano grazie alla capacità di operare a livello transfrontaliero e all’interconnettività, sono alimentate dalla labilità dei confini tra mondo fisico e digitale e sfruttano le disparità sociali ed economiche”.

This entry was posted on Monday, June 19th, 2023 at 8:30 am and is filed under Porti
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.