

Cyber security nei terminal portuali: “Lo Stato deve contribuire”

Sia Luigi Merlo (Federlogistica) che Vito Tototrizzo (Fise Uniport) richiamano un'intervento pubblico per sostenere gli investimenti necessari a prevenire i rischi di attacchi in banchina

DI REDAZIONE SHIPPING ITALY

15 FEBBRAIO 2022

[STAMPA](#)



“Il vero e unico faro per programmare e gestire i processi di innovazione tecnologica nei porti

sono le Autorità di Sistema Portual. È venuto il momento di affrontare, con serietà e concretezza e quindi nella gestione delle risorse del Pnrr, le tematiche relative all'innovazione tecnologica e alla digitalizzazione, dalle quali dipende la sicurezza così come l'efficienza e la competitività dei porti, ma anche dell'intera catena logistica”. Lo ha detto Luigi Merlo, presidente di Federlogistica-Conftrasporto, anticipando i temi in discussione nel corso del webinar organizzato da Assarmatori e Fise Uniport dal titolo ‘Cybersecurity nell’ambito marittimo – portuale’.

Secondo Merlo i tempi sono stretti: “Il 2022 sarà l’anno chiave con l’entrata in vigore della Direttiva Europea Nis 2 sulla sicurezza delle reti e dei sistemi informativi. Una direttiva che estenderà il raggio di azione in molti settori delicati tra i quali i trasporti e i porti, amplierà gli obblighi non solo alle grandi imprese ma anche a quelle medie e prevederà sanzioni elevate per chi non si adegua”. Per il vertice di Federlogistica “le risorse del Pnrr per la digitalizzazione devono quindi essere impiegate per aiutare le imprese ma anche le Autorità di Sistema Portuale a strutturarsi. È il caso di ricordare che le stesse AdSP si trovano a far fronte a carichi di lavoro rilevanti per la progettazione e l’implementazione delle opere da realizzare; e proprio in questo scenario devono poter contare su sistemi inviolabili, introducendo da subito la figura del cyber manager”.

Per il Presidente di Federlogistica-Confrtrasporto il rischio di attacchi hacker non è un'ipotesi aleatoria, è invece "terribilmente concreto". Solo un percorso di digitalizzazione che sfoci rapidamente in Cyber Security Assessment e quindi nell'impiego dei relativi piani di gestione del rischio cyber "può consentire un salto di qualità non più rinviabile".

Dello stesso avviso è parso Vito Totorizzo, vicepresidente di Fise Uniport, che intervenendo al webinar ha detto: "C'è sempre una falla dove i pericoli e le minacce informatiche possono insinuarsi. I costi e i danni potenziali sono elevatissimi, soprattutto per i grandi terminal perché anche solo con una piccola o involontaria falla ci si espone a rischi di attacchi rilevanti. Anche semplicemente aprendo un file che non si riteneva preoccupante".

Totorizzo ha evidenziato la vulnerabilità del fattore umano come fattore di rischio numero uno: "Anche il più modesto dei lavoratori potrebbe essere la chiave per far accedere gli hacker ai sistemi informatici".

A proposito della questione dei costi il terminalista barese la pensa come Merlo: "Siccome la battaglia è di interesse pubblico bisognerebbe trovare il modo di coinvolgere lo Stato ai fini di contribuire a migliorare i sistemi (che sono onerosissimi per i piccoli terminal, un po' meno per i grandi). È essenziale che il pubblico faccia la sua parte. Ogni azienda, in funzione delle proprie capacità economiche, deve organizzarsi. I grandi terminal non possono limitare solo a pochi addetti l'accesso al sistema informatico aziendale. Mi auguro che l'importanza della materia richiami lo Stato a trovare misure adeguate".