

AdSp a rischio di cyber attack: correre ai ripari

Merlo auspica risorse del Pnrr per un intervento globale sulla sicurezza



Pubblicato

il giorno

14 Febbraio 2022

Da

[Redazione](#)



ROMA – Non è un caso se nel mondo importanti scali marittimi, come Barcellona o San Diego, per la loro centralità e le funzioni di regia complessiva, siano stati oggetto di cyber attack, e in Italia il vero e unico faro per programmare e gestire i processi di innovazione tecnologica nei porti sono le Autorità di Sistema portuale.

Il commento arriva da **Luigi Merlo**, presidente di Federlogistica-Confrtrasporto che chiede, alla luce dei fatti, che le stesse AdSp siano dotate di risorse, anche professionali, che consentano loro di gestire i processi di digitalizzazione e affrontare i cyber risk, anche per l'intera comunità portuale che governano".

Le risorse del Pnrr dovrebbero secondo il presidente andare anche in questa direzione, "affrontando con serietà e concretezza, 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".

È palese la necessità di velocizzare i progetti se è vero che durante quest'anno entrerà in vigore la Direttiva Europea Nis 2 sulla sicurezza delle reti e dei sistemi informativi.

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.

"Il sistema logistico e portuale italiano -continua Merlo- non può farsi trovare impreparato.

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”.

Un nuovo modo di fare governance passa inevitabilmente per la trasformazione digitale, così che si possano rendere le azioni delle Authority sempre più in linea con gli obiettivi degli armatori, delle imprese e di tutti gli stakeholder che interagiscono nel mondo portuale italiano.

“Ma ora sono necessarie le risorse non solo economiche, ma anche umane e professionali, senza le quali il processo di digitalizzazione continuerebbe a caratterizzarsi, come accaduto per troppo tempo, in slogan e non in fatti concreti”.

Il rischio di attacchi hacker, come quelli subiti da molti porti nel mondo, non è un'ipotesi aleatoria, ma “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”.