Shipping Italy
Il quotidiano online del trasporto marittimo

Cyber-resilienza e trasporto marittimo: una sfida per l'economia globale

Nicola Capuzzo · Saturday, October 18th, 2025

*Contributo a cura di Gianluca Dini e Martina Neri **
** Polo Universitario "Sistemi Logistici" – Università di Pisa – Dipartimento di Ingegneria dell'Informazione*

La crescente digitalizzazione dei trasporti marittimi ha aumentato esponenzialmente efficienza e connettività, ma ha reso il settore più vulnerabile agli attacchi informatici. Un recente studio evidenzia come la cyber-resilienza, più che la sola cyber-sicurezza, sia ormai la condizione essenziale per garantire continuità operativa e stabilità economica globale.

Il trasporto marittimo rappresenta innegabilmente uno dei pilastri dell'economia contemporanea. Ad oggi circa l'80% del volume e il 70% del valore delle merci scambiate a livello globale viaggiano via mare. Sono quattro i grandi operatori – MSC, Maersk, CMA CGM e COSCO – che controllano oltre metà del mercato dei container (57,4%). Si tratta dunque di un settore strategico, non solo per la logistica, ma per la stabilità delle catene di approvvigionamento e, di conseguenza, anche e soprattutto per gli equilibri economici internazionali.

La progressiva digitalizzazione delle infrastrutture marittime e portuali ha reso il settore più efficiente, ma allo stesso tempo maggiormente esposto a minacce informatiche. I costi medi causati da un attacco informatico hanno raggiunto, secondo gli ultimi report, 550.000 $, con un raddoppio dal 2022 al 2023. Nello specifico, si stima che i soli porti siano vittime di almeno 12 attacchi informatici al giorno, con richieste di riscatto che superano la media dei 3 milioni di dollari. Alcuni porti estremamente rilevanti, come quelli di Anversa, Rotterdam e Barcellona, sono caduti vittima di attacchi informatici.

Per il settore marittimo più in generale, un caso emblematico è quello che ha coinvolto la compagnia danese Maersk nel 2017, quando il ransomware NotPetya paralizzò in poche ore migliaia di server e computer, determinando il blocco delle operazioni in numerosi scali internazionali. Gli effetti a cascata dell'attacco impattarono sull'intera catena logistica globale e servirono diversi mesi per il ripristino totale dell'operatività.

Verso un nuovo paradigma: dalla sicurezza alla cyber resilienza

Di fronte a minacce di tale portata e sempre più numerose, il tradizionale paradigma della cybersecurity, volto principalmente alla prevenzione, risulta ad oggi insufficiente. Si va sempre più affermando invece il concetto di cyber-resilienza, intesa come capacità non solo di resistere a un attacco, ma anche di garantire la continuità operativa, reagire tempestivamente e adattarsi alle nuove condizioni, in un'ottica di miglioramento continuo. Il focus si sposta, inoltre, da un orientamento prevalentemente tecnologico, a uno multidisciplinare che comprenda aspetti manageriali ed organizzativi.

Uno studio condotto dagli autori, recentemente presentato alla conferenza internazionale IEEE Cyber Humanities, ha analizzato, attraverso più di 90 fonti documentali, otto attacchi significativi avvenuti tra il 2017 e il 2023. La ricerca, disponibile su richiesta presso gli autori, si è focalizzata sia su grandi compagnie di navigazione, cioè Maersk, MSC, CMA CGM e COSCO, sia su organizzazioni con focus non direttamente armatoriale, quali il Porto di Lisbona, la DNV (ente di certificazione), la Swire Pacific Offshore e persino l'Organizzazione Marittima Internazionale (IMO).

L'analisi si è basata sul framework di Dupont et al., che propone dodici misure di cyber resilienza ripartite in tre fasi temporali (prima, durante e dopo l'incidente informatico), e su due dimensioni organizzative (strategica e operativa).

Risultati principali

Alcuni risultati rilevanti che emergono dallo studio emergono riguardano:

• *Tipologia di attacchi ed effetti a catena*: la quasi totalità degli attacchi è di tipo ransomware o, più in generale, malware, spesso imputabili all'errore umano. Per molti degli attacchi, il periodo necessario per tornare all'operatività totale si è assestato sulle due settimane, e nei casi più estremi anche mesi. Gli effetti a cascata si sono propagati sull'operatività dei terminal, filiali sussidiarie, dipendenti e clienti.

• *Maggiore maturità delle compagnie di spedizione*: gli armatori oggetto di studio dispongono di risorse e competenze interne più sviluppate rispetto ad altre organizzazioni del settore. Maersk, ad esempio, conta oltre 300 addetti dedicati alla cybersecurity.

• *Aree critiche individuate*: tra queste figurano la carenza di strumenti per individuare precocemente minacce e vulnerabilità (situational awareness), e la lentezza della risposta operativa in caso di attacco. In particolare, emerge una limitata attenzione alla gestione post-incidente, vista la scarsità di meccanismi di apprendimento (ad esempio nuove metodologie di formazione o key performance indicator), elemento fondamentale per trasformare l'esperienza di un incidente in un miglioramento strutturale di lungo periodo.

Implicazioni per il settore

La crescente esposizione a minacce informatiche conferma la necessità sempre più imperativa di considerare il trasporto marittimo come infrastruttura critica, come già previsto dalle direttive europee e dalle linee guida dell'IMO. A tal fine, occorre però un approccio integrato che coinvolga governance, investimenti tecnologici, formazione del personale ed ampia cooperazione e coordinazione tra attori pubblici e privati.

Gli autori dello studio propongono quindi tre direttrici prioritarie:

1. *Rafforzare la consapevolezza*, soprattutto attraverso formazione del personale, anche grazie ad attività di simulazione.
2. *Garantire tempi di risposta più rapidi*, istituendo e garantendo la presenza di team di emergenza multidisciplinari capaci di agire in poche ore.

3. *Sviluppare pratiche strutturate di knowledge management*, affinché le esperienze maturate in seguito a un attacco diventino patrimonio condiviso e base per nuove misure di prevenzione.

Conclusione

Il trasporto marittimo si trova oggi al crocevia tra tradizione e innovazione. Alla solidità delle rotte commerciali si affianca la crescente dipendenza dai sistemi digitali, la cui vulnerabilità ne governa il funzionamento. In tale contesto, la cyber-resilienza non deve essere interpretata come un costo accessorio, bensì come condizione imprescindibile per garantire l'operatività e la stabilità economica globale.

Condizione sempre più imprescindibile è quindi un approccio che integri prevenzione, reazione e apprendimento, che potrà consentire all'intero settore di affrontare le sfide di un contesto sempre più interconnesso, nel quale un singolo incidente informatico può avere effetti dalla portata globale.

This entry was posted on Saturday, October 18th, 2025 at 10:00 am and is filed under Economia
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.