Shipping Italy
Il quotidiano online del trasporto marittimo

Cyber security in ambito marittimo-portuale: “In Italia servono maggiori investimenti”

Nicola Capuzzo · Tuesday, February 15th, 2022

La cyber security in ambito marittimo-portuale è stato il tema al centro del webinar organizzato da Assarmatori e Fise Uniport durante il quale **Stefano Beduschi (Italia Marittima)** ha sottolineato la necessità di uno sforzo maggiore a livello di operational technology. “Serve uno sforzo anche da parte dell’amministrazione” ha detto, specificando di fare riferimento “ad esempio al Gps che è uno dei potenziali rischi dell’It dove poco possono fare gli armatori ma che bisognerebbe strutturare in maniera diversa da parte delle amministrazioni”.

Secondo il dirigente della compagnia di navigazione triestina “mentre il bordo, le navi, hanno dovuto fare questo sforzo, non tutti i settori interessati allo shipping sono stati obbligati a occuparsi del rischio cyber. Non è stato fatto altrettanto per tutti gli uffici e le attività che si interfacciano con le navi e possono portare pericoli legali alla cybersecurity”. Va ricordato infatti che dal 1° gennaio 2021 è obbligatorio per le navi avere una certificazione che comprovi la valutazione dei rischi cyber nell’ambito del proprio sistema Sms (Safety Management System).

Particolarmente d’impatto è stato l’intervnto di **Giacomo Speretta (Leonardo)** che ha spiegato come “gli attacchi informatici sono finalizzati a riscatti economici; è un mercato purtroppo. Non sono “diretti solo ai grandi gruppi” e le navi in particolare “sono viste come dei grandi data center. Gps e sistemi di controllo della navigazione sono oggetto di vulnerabilità”.

Speretta ha sottolineato che “spesso dietro al buon successo di un attacco cyber c’è un errore umano, scarsa formazione o disattenzione. Un’azione che espone l’azienda al rischio”. Per comprendere meglio le dimensioni del fenomeno aiuta l’esempio portato a proposito dell’attacco a Maersk “avvenuto a causa dell’obsolescenza dei sistemi informativi” e che “ha generato un danno per l’azienda da 250-300 milioni di dollari”. In quel caso tutto ha avuto inizio con l’apertura di un file malevolo da parte di un dipendente”. Ex post il gruppo danese ha avviato un accurato percorso di formazione e awareness all’interno della propria forza lavoro.

Uno degli altri case study portati da Leonardo ha mostrato come un flusso di attacco cyber a un’azienda può avvenire anche attraverso una macchietta del caffè collegata a una rete aziendale informatica aperta.

“Nel settore dei trasporti non c’è sicuramente un’attenzione adeguata ai rischi informatici, servono

investimenti e lavorare su una cultura cyber, implementare architetture per proteggere il sistema informatico e formare il personale (anche nel rapporto con l'indotto)" ha concluso Speretta annunciando che Leonardo inaugurerà a breve una sua Cyber Security Academy.

Giorgio Volta (Università degli studi di Genova), trattando il tema della security governance del sistema portuale, ha posto l'accenti sulle scalate ostili crescenti dal 2012 in poi nei confronti di aziende strategiche con conseguente attenzione crescente al Golden Power anche da parte dell'Italia non solo. "L'organizzazione di un porto – ha spiegato Volta – è molto articolata e ricca di interazioni fra le società presenti nell'ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance".

Orietta Campironi ha infine portato l'esperienza della compagnia di navigazione **Ignazio Messina & C.**, di cui è Chief Information Officer, individuando tre fattori fondamentali nella propria roadmap in matera di cyber security. Un primo fattore tecnico, "volto al consolidamento del sistema tecnico di sicurezza aziendale; un secondo normativo, riguardante "la regolamentazione sui rischi informatici che guida la risk analysis e le norme che sono d'auto per stabilire le misure da attuare". A questo proposito Campironi ha sottolineato che "talvolta le misure sono complesse e difficilmente adattabili all'eterogeneità di alcuni casi concreti".

Il terzo è il fattore umano che "spesso è sfruttato dagli attori malevoli. Se su questo fronte non si fanno azioni mirate gli strumenti tecnologici sono inutili" ha affermato. "Occorre dedicare molto tempo e dare molta importanza al processo di formazione e di apprendimento continuo".

N.C.

This entry was posted on Tuesday, February 15th, 2022 at 1:00 pm and is filed under Politica&Associazioni
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.