Shipping Italy
Il quotidiano online del trasporto marittimo

Cyber security e shipping: i rischi spiegati dall'avv. Vergani (BonelliErede)

Nicola Capuzzo · Wednesday, January 1st, 2020

Contributo a firma di Enrico Vergani, of counsel e leader del Focus Team Shipping and Transport di BonelliErede

Qual è lo stato dell'arte attuale circa la normativa in tema cybersecurity in ambito shipping?

Un'occasione per fare il punto è stata la Safety 4 Sea London Conference, tenutasi il 28 marzo di quest'anno. Il quadro che ne è derivato può sintetizzarsi in tre punti:

- non si hanno notizie di ufficiali di attacchi cyber alla nave in quanto tale, quindi agli apparati propulsivi, di governo e di controllo della nave;
- è del tutto assente un corpo normativo primario specificamente dedicato al settore dello shipping, sebbene le attività svolte da compagnie di navigazione trovino la loro disciplina in normative sviluppate a livello generale quale, in ambito di Unione Europea, il GDPR – General Data Protection Regulation e la Direttiva NIS – Network Information Security, cui l'Italia ha dato esecuzione con il DLGS 18 maggio 2018, n. 65;
- non è attualmente prevista, a livello internazionale, una normativa dedicata al fenomeno prima del gennaio 2021, data in cui dovrà entrare in vigore – secondo le indicazioni espresse dall'IMO – l'integrazione al Capitolo IX della Convenzione Solas, dedicato espressamente al fenomeno della Cyber Security.

Dal punto di vista degli operatori del settore, quali sono i maggiori rischi per essi derivanti da possibili attacchi e criticità di cybersecurity?

Nell'immaginario collettivo la scena è quella della nave "hackerata" e usata come uno strumento di distruzione. Immagine suggestiva ma piuttosto lontana dai rischi concreti connessi al nostro settore. Fortissimo è invece il rischio di danni economici legati all'interruzione del business (di grande rilievo l'attacco sferrato ai sistemi informatici di Maersk nel 2017) in presenza di un attacco cyber e, soprattutto, a seguito della successiva, repentina, chiusura del sistema informatico a causa dell'attacco.

Quali possono essere i risvolti e gli impatti economico-finanziari dei rischi sopra indicati?

La perdita di business conseguente all'interruzione del servizio è il dato che appare più immediato. La carente protezione dei dati e della privacy del cliente/consumatore è un altro settore di estremo rilievo. Recentissima (comunicato stampa del 4 dicembre scorso) è l'apertura da parte dell'AGCM di un'istruttoria su diversi gestori telefonici per una pratica aggressiva per fornitura non richiesta di servizi telefonici a pagamento (molto salati) connessi al roaming marittimo. In questo caso diversi operatori nel settore dei trasporti marittimi di linea sono stati anch'essi coinvolti a fronte di una possibile omissione di informativa (e, forse, anche carenza di protezione dei passeggeri a fronte di un servizio che scattava in automatico).

Poi c'è il tema connesso ai costi di coperture assicurative dedicate al fenomeno cyber risk, ovvero alla necessità di estensione delle attuali coperture le quali, tendenzialmente, nella propria configurazione tradizionale escludono del tutto il cyber risk. Anche su questo aspetto specifico la sensazione è di navigare ancora a vista, in attesa che si consolidino dei dati di riferimento per la quotazione del rischio e l'adozione degli strumenti assicurativi più appropriati. C'è molto fermento, tuttavia, è questo è bene.

A suo avviso, gli operatori del settore oggi che livello di consapevolezza dimostrano circa i rischi legati alla cybersecurity?

Il 19 dicembre 2011 l'ENISA (European Network Information Security Agency), agenzia dell'Unione Europea dedicata al fenomeno della sicurezza informatica aveva rilasciato un rapporto sulla consapevolezza del rischio nel settore marittimo, concludendo laconicamente che "*awarness is currently low to non-existant*". Una consapevolezza limitata in effetti si rinviene ancora in parte degli operatori, sebbene forte è la sensazione che il vento stia cambiando.

Infine, come dovrebbe evolvere il quadro normativo attuale per il settore sotto il profilo della cybersecurity?

Mi ricollego alla risposta precedente per sottolineare come, oltre che nel quadro normativo di riferimento, il cambiamento deve essere culturale. La commistione tra contatti pubblici e privati, l'uso dei social da postazioni di lavoro, l'identità delle password (privata e business), l'uso ed abuso delle storage unit sono comportamenti che, prima ancora che vietati, debbono essere banditi dalla nostra cultura nell'impiego di supporti informatici. La normativa molto può fare – ed attendiamo con curiosità la prossima circolare del Comando Generale delle Capitanerie di Porto dedicata proprio alla cyber security a bordo – ma il cambiamento parte dall'informazione, consapevolezza e cultura aziendale. Come per la sicurezza e la manutenzione programmata, in ultima analisi un ulteriore incremento nella qualità.

This entry was posted on Wednesday, January 1st, 2020 at 12:07 am and is filed under Interviste
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.