Shipping Italy
Il quotidiano online del trasporto marittimo

Shipping, cyber security e risk management: un approccio olistico

Nicola Capuzzo · Friday, October 9th, 2020

*Contributo a cura di Enrico Vergani **

** Of counsel e leader del Focus Team Shipping and Transport di BonelliErede*

Il mese di settembre si è chiuso con diversi avvenimenti che hanno ancora una volta evidenziato l'opportunità di una seria riflessione sull'impatto del cyber risk nel mondo dello shipping e delle merci viaggianti e dei servizi accessori all'impresa, in particolare l'assicurazione.
Il terzo grande liner operante nel traffico container, CMA CGM, dopo Maersk e MSC, è stato oggetto di un attacco da parte di hacker, questa volta particolarmente mirato e, secondo alcune fonti, accompagnato da una vera e propria richiesta di riscatto (ransomware). Alcuni giorni più tardi è l'IMO – International Maritime Organisation, l'agenzia delle Nazioni Unite competente nel settore marittimo, che diventa oggetto di un attacco informatico ai propri sistemi. La stessa IMO che ha traguardato al gennaio 2021 l'adeguamento della normativa SOLAS al fenomeno del cyber risk. Scontato osservare che "i cattivi" sono arrivati prima. In ultimo, il 1° ottobre 2020 l'OFAC – Office of Foreign Assets Control, dipendente dal Dipartimento del Tesoro degli Stati Uniti, emana una propria pubblicazione sul rischio di sanzioni nell'ipotesi di pagamento di riscatto a favore di hacker che ricadano nel novero dei Special Designated Nationals (SDN), ovvero dell'esecuzione di attività che faciliti il pagamento di un ransomware, con la possibilità per i soggetti coinvolti di essere colpiti da sanzioni, con profili che si estendono alla stessa validità delle coperture assicurative poste in essere.
Il documento, reperibile sul sito del Dipartimento del Tesoro (link), cita il rapporto sul crimine informatico rilasciato dall'FBI relativo agli anni 2018 e 2019, il quale evidenzia un incremento del 37% del fenomeno del ransowmware e del 147% dei danni economici conseguenti agli attacchi cibernetici.
Per quanto riguarda il divieto di pagamento del riscatto, OFAC prosegue nella propria disamina sottolineando che numerosi malicious cyber actors sono ormai inseriti nella lista dei SDN, mentre un numero considerevole di attacchi può essere connesso a Paesi oggetto della normativa sulle sanzioni internazionali (Russia ed Iran, soprattutto). L'obiettivo dell'irrigidimento chiaramente manifestato dall'Agenzia statunitense trova le proprie ragioni non solo nella prevenzione speciale, a evitare che comportamenti criminosi divengano

sempre più remunerativi, alimentando un'escalation dei medesimi, ma altresì nell'intento di rafforzare il sistema sanzionatorio anche con riferimento alle infrastrutture non fisiche.
La chiara indicazione espressa da OFAC per gli operatori economici è quella di non confidare sull'automatica operatività della copertura assicurativa che preveda il pagamento del riscatto, chiarendo fin da subito che eventuali licenze in deroga verranno valutate caso per caso con un'espressa presumption of denial, adottando piuttosto all'interno di ciascuna realtà produttiva uno strutturato sanction compliance program.

Le riflessioni che le recenti vicende dovrebbero suscitare tra gli operatori del settore dello shipping e dei servizi assicurativi sono molteplici. Ne individuiamo almeno un paio. Per gli assicuratori, i broker e tutti i service provider nel settore del cyber risk che offrano i propri servizi nel settore dello shipping e della logistica emerge evidente la necessità – spesso non percepita in maniera sufficiente – di valutare i rischi propri del mercato in cui operano, tra cui la necessità di un diffuso controllo del possibile impatto da parte del sistema sanzionatorio internazionale, specialmente di matrice USA. Più volte sottolineiamo che lo shipping è una "bestia particolare" (meravigliosa ma complessa) che richiede il rispetto e la conoscenza delle proprie peculiarità: così come gli istituti finanziari hanno imparato, spesso a proprie spese, che finanziare una nave non necessariamente equivale ad assumere il rischio di uno stabilimento di terra, allo stesso modo coperture assicurative, procedure, sistemi di protezione debbono essere configurati su misura con riferimento al business e alla struttura aziendale cui accedono.

Occorre dunque un approccio che tenga conto delle peculiarità del mercato e sia al tempo stesso olistico, capace di coniugare i diversi aspetti della vita in azienda in cui potrebbe manifestarsi il rischio di un cyber attack, la necessità di contenerlo e di ridurre al contempo i danni da business interruption. Il che sempre più coinvolge complesse questioni di governance per cui la protezione contro il cyber risk (e la gestione delle conseguenze dell'attacco che comunque prima o poi accadrà) non può essere affidata a una divisione dell'IT (o allo stesso IT "nei ritagli di tempo") ma deve passare dalla competenza di una semplice unità di supporto a quella propria di un autonomo settore di business, capace di farsi comprendere da interlocutori non tecnici, apprezzare le peculiarità dell'industria cui il cyber service accede e comunicare in un linguaggio business to business, capace di allineare gli obiettivi della strategia cyber security a quelli dell'azienda.

La sfida è aperta e si rinnova ogni giorno. E il settore dello shipping, come spesso accade, potrebbe essere chiamato a guidare il cambiamento.

This entry was posted on Friday, October 9th, 2020 at 10:30 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.