OSSERVATORIO SULLA SICUREZZA MARITTIMA

Maritime Cyber Security

ANALISI

L'attacco cyber alla Mediterranean Shipping Company del 9 aprile 2020

MAGGIO 2020

Società Italiana di Intelligence

Francesco Chiappetta - Andrea Sberze

L’attacco cyber alla Mediterranean Shipping Company del 9 aprile 2020

Società Italiana di Intelligence
c/o Università della Calabria, Cubo 18-b, 7° piano
via Pietro Bucci
87036 Arcavacata di Rende (CS) – Italia

https://www.socint.org

ISBN: 979-12-80111-23-4

INDICE

PREMESSA

La dimensione marittima della sicurezza internazionale è una priorità, se solo si voglia concentrare l'attenzione sull'importanza strategica della logistica marittima. Il mare è superficie di trasporto, ma se non è opportunamente considerato e difeso può rappresentare un ostacolo al libero fluire delle merci e delle persone: è spazio che divide e non collegamento per unire.

Certo, la percezione della sicurezza cambia perché a mutare sono i fattori che determinano il contesto di volta in volta considerato. Per questo motivo, senza farci illusioni, non esiste una sicurezza totale. Tuttavia, attraverso la consapevolezza delle nuove sfide che dobbiamo affrontare, non ultima quella tecnologica, possiamo sicuramente farci un'idea sulle priorità e innescare il dibattito per meglio gestire le risorse di cui disponiamo. Per questo motivo, uno dei principali temi trattati dall'Osservatorio sulla Sicurezza Marittima[1] è quello connesso agli studi dei rischi e delle minacce informatiche che si realizzano nel dominio marittimo[2]. Una di-

1 L'Osservatorio sulla Sicurezza Marittima è stato istituito nel 2019 presso l'Università degli Studi della Calabria nell'ambito del Laboratorio di Intelligence del "Centro di Documentazione Scientifica sull'Intelligence", che tra l'altro promuove il Master di II livello in Intelligence diretto dal Prof. Mario Caligiuri (https://www.intelligencelab.org/losservatorio-sulla-sicurezza-marittima/).

2 Con la digitalizzazione in ambito marittimo e portuale, la sicurezza cibernetica è argomento di primaria importanza, anche e soprattutto per il consolidamento di un approccio teso ad analizzare le criticità di un'industria potenzialmente vulnerabile all'utilizzo improprio delle tecnologie impiegate a bordo nave o nelle infrastrutture portuali. A titolo d'esempio, si suggerisce la lettura del documento pubblicato da BIMCO, CLIA, ICS, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, *The Giudelines on Cyber Security Onboard Ships,*

mensione della sicurezza cibernetica in un ambito particolare e specifico quale quello dello *shipping*, la cui consapevolezza e le strategie di contrasto rappresentano un fattore strategico – sia per le Compagnie di navigazione e conseguentemente pe la propria Flotta, sia per le infrastrutture logistiche portuali – per una economia di un Paese come l'Italia estremamente dipendente dai trasporti marittimi[3].

In un tale scenario, l'esame e l'analisi, laddove possibile, di specifici casi, svolto in particolare attraverso gli strumenti culturali che la ricerca informativa offre, consente di fornire interessanti elementi di approfondimento su cui poter incentrare lo studio scientifico dell'intelligence mirato appunto al dominio marittimo[4].

Obiettivo di questo breve lavoro è quindi quello di evidenziare alcuni aspetti caratteristici emersi in occasione di un recente at-

---

version 3 https://www.maritimecybertraining.online/sheet/90083647-bimco. Vedi anche H. BOYES, R. ISBELL, *Code of Practice – Cyber Security for Ships*, *IET Standards*, *Department for Transport*, 2017. Per la sicurezza cibernetica concentrata sulle infrastrutture portuali, vedi *Port Cybersecurity - Good practices for cybersecurity in the maritime sector*, pubblicata dall'*European Union Agency for Cybersecurity* (ENISA) in novembre 2019, https://www.maritimecybertraining.online/sheet/department-for-transport-iet-standards.

3 Con la cd digitalizzazione in ambito marittimo, non passa inosservata l'attenzione delle assicurazioni marittime nei confronti delle analisi focalizzate sul rischio cibernetico. Per maggiori informazioni vedi, per esempio https://www.-maritimecyberadvisors.com/. Nello specifico delle infrastrutture portuali, evidenziamo il lavoro pubblicato da *Lloyd's of London*, *Cambridge Centre for Risk Studies, Nanyang Technological University*, *Shan Attack: Cyber risk in Asia ports*, 2019.

4 Interessante notare come l'approccio analitico nei confronti della sicurezza cibernetica in ambito marittimo stia diventando un focus sempre più importante anche a livello accademico. Si segnala, per esempio, la nascita del *Maritime Cyber Threats research group,* presso la *University of Plymouth*, https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group.

tacco cyber subito da un'importante Compagnia di Navigazione di respiro internazionale leader a livello mondiale nel trasporto container. Uno studio mirato, senza tuttavia entrare nel dettaglio di elementi prettamente tecnici, avente come scopo quello di mettere in evidenza specifiche evidenze nelle dinamiche secondo le quali si è sviluppato l'incidente, quali sono le strategie messe in campo dalla Compagnia e, in linea generale, valutare alcuni aspetti di *governance* nella gestione del rischio informatico.

Scopo finale è, infine, quello di rendere disponibile un documento di lavoro – nello specifico un cd. "caso di studio" – modo disporre di materiale a disposizione per le lezioni e le conferenze sul tema della *Maritime Cyber Security* tenute nell'ambito del Laboratorio di *Cyber intelligence* del Master in Intelligence previsto dai piani di studio dell'Università degli studi della Calabria[5].

5 Cfr.: https://www.intelligencelab.org/losservatorio-sulla-sicurezza-marittima/.

INTRODUZIONE

Il **9 aprile 2020** il sito web della *Mediterranea Shipping Company* (MSC)[6], Società leader mondiale per il trasporto marittimo in particolare containerizzato, per circa 10 ore risultava non disponibile. L'inconveniente, come riportato alla pagina web del sito (Fig. 1) – «msc.com» – si è protratto per circa 6 giorni per poi essere rispristinato il **15 aprile**.

Fig. 1 *- comunicato presente sul sito web di MSC (cargo) durante il verificarsi dell'inconveniente.*

Gli elementi che seguono sono il prodotto di uno studio dell'evento attraverso la selezione e la lettura di fonti essenzial-

6 *MSC Mediterranean Shipping Company* – Azienda globale attiva nel settore delle spedizioni e della logistica. Presente in 155 paesi, MSC facilita il commercio internazionale tra le principali economie mondiali e tra i mercati emergenti di tutti i continenti. (https://www.msc.com/ita).

mente aperte ed adeguatamente validate. Gli elementi raccolti alla data di stesura di questo documento consentono, pertanto, di sviluppare una breve analisi dell'attacco informatico subito e procedere a principali considerazioni di carattere generale inerente la specifica dimensione marittima.

ELEMENTI TEMPORALI DELL'ATTACCO

La prima fonte sulla rete a dare notizia dell'incidente – già il 9 aprile – è stata da parte di Lars Jensen, analista di *SeaIntelligence Consulting*, il quale ha subito parlato di un attacco cyber andato a buon fine[7].

Numerosi siti web (vedi riquadro a pag. 10), internazionali e nazionali, già dal 10 di aprile fino al 15 aprile, ne hanno poi riportato la notizia non escludendo ma neanche confermando un possibile attacco informatico in corso.

La Società, su Twitter, ha inizialmente confermato il disservizio parlando di un problema legato al proprio data center di Ginevra; poi, però, ha reso noto di non poter escludere l'ipotesi di un "malware" concentrato sui sistemi informatici presso il proprio Quartier Generale e che aveva influito sulla disponibilità di alcuni servizi. Al momento del blocco sia il sito Web globale di MSC che il sito «myMSC.com», rispettivamente il portale clienti e la piattaforma di prenotazione, sono risultati inaccessibili.

7 *SeaIntelligence Consulting* (Società danese): https://www.seaintelligence-consulting.com/about. Vedi anche il post di *Lars Jensen* su LinkedIn, https://www.linkedin.com/posts/larsjensenseaintelligence_msc-continues-to-battle-with-the-aftermath-activity-6654652670361522176-bLPp/.

ATTACCO CYBER SUBITO DALLA "MSC" IL 9 APRILE 2020

Di seguito alcuni dei siti, internazionali e nazionali, che hanno dato notizia dell'attacco:

1. Siti internazionali:
   - 09 aprile: https://www.seaintelligence-consulting.com/about
   - 10 aprile: https://www.offshore-energy.biz/msc-hit-by-suspected-cyber-attack/
   - 10 aprile: https://lloydslist.maritimeintelligence.informa.com/LL1131906/MSC-suffers-suspected-cyber-attack
   - 10 aprile: https://gcaptain.com/msc-reports-network-outage-cyber-attack-cannot-be-ruled-out/?utm_source
   - 13 aprile: https://safety4sea.com/msc-hit-by-potential-cyber-attack/?__cf_chl_jschl_tk__
   - 14 aprile: https://www.infosecurity-magazine.com/news/msc-suffers-suspected-cyberattack/
   - 15 aprile: https://www.supplychaindive.com/news/msc-outage-cyber/575900/
2. Siti nazionali:
   - 10 aprile: https://www.shipmag.it/attacco-hacker-a-msc-il-sito-della-societa-inattivo-da-piu-di-10-ore/
   - 10 aprile: https://agenparl.eu/msc-suffers-suspected-cyberattack/
   - 10 aprile: https://www.shippingitaly.it/2020/04/10/possibile-attacco-hacker-nei-confronti-di-msc/
   - 10 aprile: https://telenord.it/un-attacco-informatico-spegne-il-sito-msc

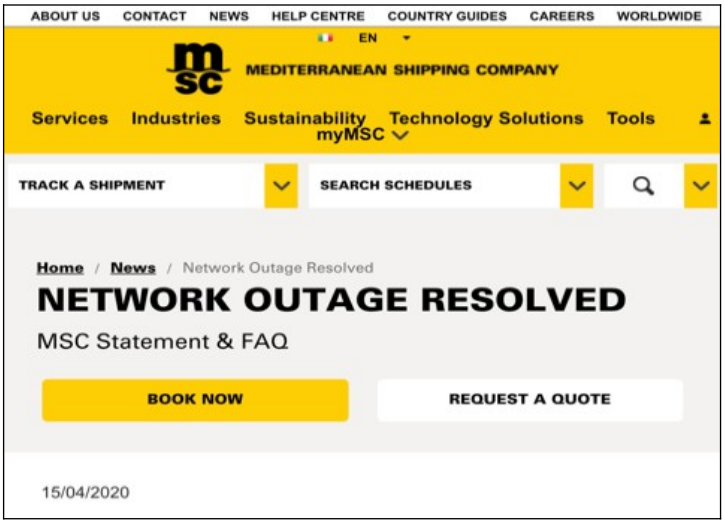
La Società ha, tuttavia, subito fornito come alternativa la disponibilità di piattaforme online di terze parti – come INTTRA, GT Nexus e CargoSmart – nonché collegamenti direttamente tramite i propri rappresentanti MSC utilizzando metodi più tradizionali come telefono o e-mail personali.

Successivamente, ancora su Twitter, MSC ha comunicato «*di chiudere i server nella sede come prima misura di sicurezza, poiché la sicurezza è la nostra priorità assoluta*» per poi precisare di «*monitorare e valutare la situazione, lavorando per il pieno recupero nel più breve tempo possibile*». Inoltre, ha voluto rassicurare

che «*la rete mondiale di agenzie sta funzionando e i nostri agenti locali stanno supportando i clienti per tutti i servizi come avviene abitualmente*»; ha infatti inteso precisare che tutte le agenzie marittime locali del gruppo come tutti i propri Uffici erano comunque rimasti pienamente operativi[8]. Il 12 aprile, sempre via Twitter, la Società sembrava fiduciosa di intravedere a breve una soluzione, affermando che il problema sarebbe stato risolto a breve. Il **15 aprile 2020**, dopo circa 6 giorni dall'evento, MSC ripristinava i servizi del proprio sito istituzionale (Fig. 2) e subito pubblicava uno proprio rapporto – "MSC STATEMENT & FAQ" – con il quale andava a chiarire le dinamiche dell'inconveniente fornendo una serie di risposte a specifiche domande preparate.

In sintesi, la Società ha confermato di essersi trattato effettivamente di un attacco cyber. Un "***malware***" basato su di una cd. «*vulnerabilità mirata ingegneristica progettata*». Ha comunque affermato che l'incidente si è limitato ad un numero esiguo di «*physical computer systems*» esclusivamente presso la sede di Ginevra, con un impatto definito «***limitato***» per il quale sono stati adottati i protocolli interni riguardanti la sicurezza, le comunicazioni e le transazioni commerciali. MSC ha anche affermato di aver condiviso con i propri partner tecnologici, secondo gli standard del settore, le caratteristiche del *malware* sofferto in modo che le mitigazioni venissero rese disponibili non solo all'interno della Società. Nel predetto rapporto MSC ha comunque tenuto a precisare di non aver voluto commentare e fornire in dettaglio gli aspetti tecnici dell'attacco, dichiarando che ciò sarebbe stato «*controproducente dal punto di vista della sicurezza*».

8 In Italia, per esempio, l'Agente Generale Raccomandatario che rappresenta la *Mediterranean Shipping Company* S.A. è il gruppo "Le Navi". Vedi sito https://www.lenavigroup.it/.


ABOUT US
CONTACT
NEWS
HELP CENTRE
COUNTRY GUIDES
CAREERS
WORLDWIDE
EN
MEDITERRANEAN SHIPPING COMPANY
Services
Industries
Sustainability
Technology Solutions
Tools
myMSC
TRACK A SHIPMENT
SEARCH SCHEDULES
Home / News / Network Outage Resolved
NETWORK OUTAGE RESOLVED
MSC Statement & FAQ
BOOK NOW
REQUEST A QUOTE
15/04/2020

ANALISI

L'incidente subito il 9 aprile 2020 dalla MSC segue gli attacchi informatici che hanno colpito rispettivamente nel 2017 e nel 2018 la danese *A.P. Møller – Mærsk* e la cinese *Cosco Shipping Lines*. (vedi riquadro sotto)[9].

Con questo incidente nell'arco degli ultimi tre anni le tre principali compagnie di trasporto container a livello mondiale hanno subito un attacco informatico. Ad oggi, la *Mediterranean Shipping Company*, dopo la Società danese è, infatti, la seconda più grande compagnia marittima di container al mondo, controllando circa 570 navi pari 16% della capacità mondiale di trasporti in termini di TEU[10].

9 L'attacco cibernetico alla società A.P. Møller – Mærsk è ben descritto nell'articolo di A. GREENBERG, *The untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, 22.08.2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Per l'attacco cibernetico al gruppo COSCO vedi, C. SHEN, *Cosco Shipping targeted in ransomware attack*, Lloyd's List, 25.07.2018, https://lloydslist.maritimeintelligence.informa.com/LL1123581/Cosco-Shipping-targeted-in-ransomware-attack.

10 Si tratta dell'unità equivalente a venti piedi (acronimo appunto di *Twenty-foot Equivalent Unit*), quale misura standard di volume nel trasporto dei container, corrispondente a circa 38 metri cubi d'ingombro totale.

Gli attacchi alla A.P. Møller – Mærsk e alla COSCO Shipping Line.

Il 27 giugno 2017 la Società A.P. Møller – Mærsk, leader mondiale nei trasporti marittimi, attualmente al primo posto tra le compagnie marittime per ricavi del traffico container mondiale, in concomitanza di altri attacchi cyber, subiva una pesante intromissione ai propri sistemi informatici. La notizia veniva ripresa da molte fonti. Si è trattato, in particolare, di una intrusione cyber all'interno dei sistemi della Società con richiesta di riscatto vs. la perdita di tutti i dati (ransomware). Il virus responsabile, secondo le maggiori società di analisi, è stato individuato con il nome "Petya/NoPetya". A causa di tale attacco è stata stimata una perdita di introiti pari a circa 300 milioni di dollari dovendo, peraltro, sostenere la reinstallazione di oltre 4.000 server, 45.000 PC e circa 2.500 applicazioni, con una ripresa della piena operatività della Compagnia dopo una decina di giorni circa.

Il 24-25 luglio 2018 si è invece verificato l'attacco al gruppo COSCO (China Ocean Shipping COmpany) gestito, invece, in modo più tempestivo e presumibilmente con un minor numero di danni di cui, però, non sono noti i termini dei costi contenuti.

a. Innanzitutto l'attuale momento storico e la tempistica secondo cui l'evento si è realizzato consente di fissare alcune evidenze:
- l'attacco si è concretizzato nel bel mezzo della pandemia da COVID-19; un periodo certamente eccezionale che, dal punto di vista info-tecnologico, risulta peraltro particolarmente caratterizzato da un elevato incremento dei flussi di dati a livello globale apparso decisamente superiore alla media; una condizione probabilmente aggravata da condizioni di lavoro essenzialmente svolte sulla rete (lavoro a distanza, uso essenziale di e-mail e in molti casi delle reti

"*social*", oltre che video conferenze o telefonate collettive su piattaforme di comunicazione dedicate)[11];

- è altamente probabile/evidente che al momento dell'attacco anche per MSC erano implementate attività lavorative «a distanza», nell'ottica di una strategia industriale mirata a mantenere, anche in condizioni di crisi, una propria efficace capacità operativa. Attività quindi, e come per le maggiori società, svolte su piattaforme di comunicazione digitali e sistemi *hardware* aziendali auspicabilmente dotati di adeguati protocolli di sicurezza informatica; una condizione di lavoro a distanza tuttavia in qualche modo degradata rispetto a normali condizioni di lavoro;
- al momento dell'attacco si era nell'imminenza di un lungo WE legato alle festività pasquali, quindi una condizione evidentemente vicina ad un periodo contraddistinto da una minore presenza lavorativa presso la sede di Ginevra; elemento questo di ulteriore criticità o quantomeno di ridotta disponibilità di personale tecnico, soggetto anche alle predette modalità di lavoro a distanza, con una limitata possibilità di intervenire fisicamente e con adeguata rapidità su eventuali sistemi/hw danneggiati/bloccati.
- In base a tali elementi sembrerebbe che l'attaccante abbia individuato un periodo particolarmente favorevole dove, di massima, maggiore sarebbe risultato il grado di vulnerabilità del target. In questo senso si ritiene che il periodo prescelto per l'attacco non risulti semplicemente casuale, ma ricercato. Peraltro è noto il fatto che molti at-

11 Vedi Hellenic Shipping News, *"Cyber security amid a global pandemic"*, 07.04.2020,_https://www.hellenicshippingnews.com/cyber-security-amid-a-global-pandemic/.

tacchi informatici vengono perseguiti proprio in momenti in cui l'attenzione o la capacità d'intervento può essere meno efficace. Del resto la stessa MSC, nel report del 15 aprile, ha confermato di aver sofferto alcune difficoltà per intervenire nei giorni non lavorativi previsti per il periodo festivo. Anche questo aspetto ha certamente generato la non operatività del sito MSC per ben 6 giornate. Un momento, in definitiva, particolarmente sfruttabile da cyber criminali che appaino nelle metodologie di attacco mettere in campo strategie sempre più sofisticate.

b. L'evento è risultato concentrato e mirato sui sistemi ubicati presso il Quartier Generale di MSC a Ginevra; la Società ha, infatti, dichiarato di trattarsi come già ridordato di un attacco ***malware*** basato su di una «*vulnerabilità mirata progettata*». Questo, in linea di massima, conferma che non si è trattato di un hackeraggio diffuso e/o distribuito a più obiettivi o altre Società ma, presumibilmente, mirato solo alla stessa MSC e quindi con un ben preciso obiettivo da conseguire (vedi riquadro sotto).

(APRILE 2020) – Recentemente sempre più "mirati" appaino gli attacchi informatici subiti dalle società di shipping o anche semplicemente diretti a singole navi.

Inoltre, negli ultimi mesi contraddistinti dalla pandemia da COVID-9, secondo le maggiori società di sicurezza informatica e di intelligence, gli attacchi informatici anche nel settore marittimo risultano in particolare aumento. Gli aggressori, che secondo fonti aperte risulterebbero presumibilmente russi o dell'Europa dell'Est, prenderebbero di mira quasi esclusivamente industrie particolar-

mente sensibili alle interruzioni del trasporto marittimo.

Dryad Global's (https://dryadglobal.com/), società specializzata nell'analisi dei dati secondo strumenti di intelligence, conferma infatti che le reti criminali informatiche mirano a ricercare obiettivi delle Compagnie di Spedizione da attaccare sempre più specifici e mirati adattando ed indirizzando e-mail malevoli a determinate figure aziendali.

Tali valutazioni sembrano essere confermate anche dalla Società Red Sky Alliance (https://redskyalliance.org/s) che, settimanalmente, fornisce dati relativi agli attacchi informatici subiti dal settore marittimo; in genere si tratta di attacchi eseguiti sempre vai email (malware o pishing). Recentemente e-mail simulano addirittura l'OMS.

Riquadro – Attacchi allo shipping [fonti varie web (7)].

c. MSC, sempre nel report del 15 aprile, pur confermano di aver subito un *malware* non è voluta entrare, per ragioni pienamente comprensibili di sicurezza e riservatezza, nelle specifiche caratteristiche tecniche osservate. Tenuto conto del fatto che, come noto, esistono varie topologie di *malware* ([12]), non

12 *Malware*: contrazione di *malicious software*. È in buona sostanza un "programma" che si inserisce in un sistema informatico, generalmente in modo clandestino, con vari obiettivi come quello di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. I *software* malevoli sono divenuti, nel tempo, sempre più sofisticati. Non solo sono adattabili a qualsiasi tipologia di obiettivo, ma sono anche in grado di sfruttare vulnerabilità non ancora note (c.d. 0-day) per infettare le risorse informatiche dei target. Ciò consente a tali *software* di non essere rilevati dai sistemi di protezione e di passare praticamente inosservati. I *malware* sono in grado di celarsi nell'ambito del sistema-obiettivo, di spostarsi al suo interno, così da poterne effettuare una mappatura e propagare l'infezione. Infine, grazie agli stessi, le informazioni di interesse, prima di essere sottratte, vengono compresse e criptate per celarne l'esfiltrazione con il traffico di rete

è tuttavia chiaro che si sia trattato, ad esempio, di un *ransomware* (a fini di un profitto economico) ovvero di uno *spyware* (appropriazione di dati industriali, finanziari o comunque sensibili). La Società, inoltre, ha comunque dichiarato di non essere a conoscenza dei dati compromessi o addirittura persi e non ha fornito alcuna indicazione circa una valutazione dell'impatto economico.

d. Come conseguenza dell'attacco non sembra escludersi, almeno a livello collaterale, quello connesso ad un effetto di "danno reputazionale"[13]. Come accennato all'inizio, tra le tre grandi Compagnie di trasporto marittimo di container dopo la da-

generato dall'ordinaria attività lavorativa del *target*.

Diverse sono le tipologie di *malware*; una delle prime forme sono stati i vecchi *virus*, poi tra i più comuni vi sono i *trojan* (sw che celano il vero intento), i *worm* (sw replicanti), gli *adware* (pubblicità indesiderate), i *memo-file* (si iniettano nei processi in esecuzione modo non essere rilevabili), gli *scareware* (sw dannosi o di limitata utilità suggerita con tecniche di marketing scorretto come ad esempio quelli che propongono sw per la manutenzione del sistema operativo accompagnati da certificazioni false etc.), e poi ancora i *ransomware* o gli *spyware*.

Negli attacchi di *ransomware*, molto diffusi, l'obiettivo è il profitto con il fine ultimo di estorcere quanto più denaro possibile a più target contemporaneamente allo scopo che almeno una parte di questi vengano effettivamente raggiunti in modo efficace. Secondo un recente report di CLUSIT (https://clusit.it/) i *ransomware* sono costantemente in primo piano tra le principali minacce alla sicurezza informatica, quelli già noti evolvono mentre le forme più recenti - come ad esempio Maze - non solo cifrano i dati ed interrompono la continuità operativa dell'organizzazione colpita, ma causano anche gravi fughe di dati riservati.

Invece un *spyware* è progettato per esfiltrare informazioni riservate/sensibili da una determinata organizzazione, in genere dovrebbero colpire singoli o pochi utenti o magari uno o un limitato numero di server specifici.

13 Il rischio cibernetico, di fatto, rientra nella valutazione articolata per salvaguardare la *business continutity* e la *reputation* aziendale.

nese Mærsk e la cinese COSCO, mancava all'appello proprio la MSC.

e. Il 6 aprile, quindi solo alcuni giorni prima dell'incidente, l'amministratore delegato e presidente di MSC[14], con una lettera postata sul sito della società aveva preannunciato che una delle contromisure che la Compagnia intendeva sfruttare per fronteggiare l'emergenza e l'impatto del Coronavirus era proprio una estesa digitalizzazione dei propri servizi; ad esempio, il sistema di *booking* dei container tramite il proprio portale web. Il dubbio rimane che proprio tali dichiarazioni abbiano in qualche modo attirato l'attenzione di competitori o semplicemente *hacker* ma comunque con appropriate competenze tecniche (vds. riquadro sotto – fonti in nota[15]) per provocare un attacco che, come sopra rilevato, è risultato in ogni caso mirato.

f. Infine, dagli elementi raccolti è evidente che la Società ha comunque messo in atto protocolli di sicurezza certamente prepianificati, attivando sistemi di comunicazione alternativi che gli hanno comunque consentito, anche durante il periodo di blocco del proprio sito istituzionale, l'operatività dei movimenti e prenotazioni dei trasporti. Efficace è apparsa la comunicazione istituzionale seguita dalla Società fin dall'inizio dell'inconveniente.

---

14 https://www.msc.com/site-template/news/2020-april/covid-19-an-open-letter-from-diego-aponte?agencyPath=ita.

15 https://www.proofpoint.com/us/threat-insight/post/coronavirus-themed-attacks-target-global-shipping-concerns;_https://splash247.com/cyber-criminals-target-shipping-with-coronavirus-themed-emails/.

CONCLUSIONI

Sebbene nello scorso anno e nei primi tre mesi del 2020 non erano stati registrati attacchi informatici di particolare rilievo subiti dallo *shipping*, l'evento del 9 aprile ripropone in maniera evidente quanto il tema della *Cyber Security* debba rimanere al centro dell'attenzione dell'industria marittima. Ogni attacco, di fatto, implica una minaccia al business, con conseguenza difficilmente immaginabili considerato l'impatto economico su un mercato di per sé essenzialmente internazionale.

Una minaccia che conferma la sua efficacia anche per grandi Società armatoriali, come quelle sopra indicate, le quali certamente possono disporre di rilevanti risorse da poter dedicare sia in termini di sistemi di protezione che, soprattutto, nella formazione del proprio personale. Quest'ultimo aspetto rappresenta certamente il fattore strategico su cui puntare in quanto, alla fine, dietro ogni schermo/telefono è sempre l'operatore umano l'ultima soglia di attenzione da superare. Il problema, lungi dall'essere solo tecnico, è sostanzialmente gestionale perché nel fattore umano si individua, di fatto, una vulnerabilità.

In ultimo, come già sottolineato, è alquanto evidente che l'attacco attacco subito dalla MSC è sopraggiunto anche in un momento in cui la pandemia COVID-19 sta già mettendo a dura prova le catene di approvvigionamento globali che come più volte ripetuto si svolgono per oltre l'80% via mare. Ciò nonostante la risposta da parte dell'industria marittima, soprattutto a livello internazionale, appare alquanto compatta e coesa a sostenere la sfida

di questi mesi e in grado di assicurare una piena continuità dei trasporti marittimi.

Bibliografia e riferimenti

• BIMCO, CLIA, ICS, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, The Guidelines on Cyber Security Onboard Ships, version 3, 2018, https://www.maritimecybertraining.online/sheet/90083647-bimco.

• BOYES & ISBELL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf.

• CALIGIURI M., SBERZE A., Il pericolo viene dal Mare - Intelligence e portualità, Rubettino Editore, Soveria Mannelli, Luglio 2017.

• CHIAPPETTA F., "Sicurezza marittima informatica", Rivista Marittima Ottobre 2016, pagg.53-61.

• CHIAPPETTA F., "La Compagnia Maersk ritorna protagonista mondiale del trasporto container", Rivista Marittima Dicembre 2017, pag. 113.

• CHIAPPETTA F., "Attacco cyber alla COSCO incontra tempestive difese", Rivista Vita e Mare, Settembre-Ottobre 2018, p.5.

• CHIAPPETTA F., "Sicurezza marittima – Vecchie nuove minacce", Rivista Marittima, Maggio 2019, pagg.18-30.

• CHIAPPETTA F., "Cyber Security – Quali minacce per la Shipping Industry", Porto&Interporto, Dicembre 2019, pagg.10-12.

• ENISA (Agenzia per la Cybersecurity dell'Unione Europea), Glossary, https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/.

• ENISA – Port Cybersecurity – Good practices for cybersecurity in the maritime sector: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

• GREENBERG A., "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, 22.08.2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

• HELLENIC SHIPPING NEWS, "Cyber security amid a global pandemic", 07.04.2020, https://www.hellenicshippingnews.com/cyber-security-amid-a-global-pandemic/.

• IMO Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems, adopted on 16 June 2017.

• IMO MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management, 5 July 2017.

• LLOYD'S OF LONDON, CAMBRIDGE CENTRE FOR RISK STUDIES, NANYANG TECHNOLOGICAL UNIVERSITY, Shan Attack: Cyber risk in Asia ports, 2019, https://irfrc.ntu.edu.sg/Research/cyrim/Pages/Home.aspx.

• SHEN C., "Cosco Shipping targeted in ransomware attack", Lloyd's List, 25.07.2018, https://lloydslist.maritimeintelligence.informa.com/LL1123581/Cosco-Shipping-targeted-in-ransomware-attack.

• ZAMPIERI F., "Maritime cybersecurity e maritime cyberwarfare", Rivista Marittima Novembre 2019, pagg.14-23.

Sitografia

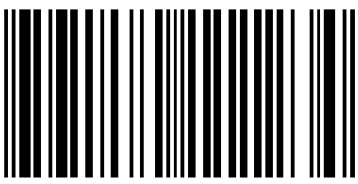
- www.clusit.it/
- www.dryadglobal.com/
- www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware
- www.facebook.com/Intelligencelabunical/
- www.gchq.gov.uk/section/mission/overview
- www.hellenicshippingnews.com
- www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx
- www.intelligencelab.org/
- www.ictsecuritymagazine.com/articoli/rischio-cyber-e-covid-19/
- www.ics-shipping.org/
- www.irfrc.ntu.edu.sg
- www.lenavigroup.it
- www.lloydslistintelligence.com/
- www.msc.com/ita
- www.maritimecybertraining.online
- www.maritimeglobalsecurity.org/
- www.marsecreview.com/about-us/
- www.ncsc.gov.uk/section/about-ncsc/what-we-do
- www.redskyalliance.org/s
- www.unical.it.
- www.wired.com

Documento ultimato il: 7 maggio 2020

GLI AUTORI

Francesco Chiappetta Ufficiale di Stato Maggiore della Marina Militare in ausiliaria dal 2016. Segue temi di Difesa e Security marittima. Docente al Laboratorio sullIntelligence del Master in Intelligence di UNICAL. Presidente dellOsservatorio sulla Sicurezza Marittima.

Andrea Sberze Studioso di terrorismo e di sicurezza marittima e portuale. Docente al Laboratorio sullIntelligence del Master in Intelligence di UNICAL. Coordinatore dellOsservatorio sulla Sicurezza Marittima.



9791280111234