



CONTINUANO GLI ATTACCHI INFORMATICI

Cybersicurezza, shipping in affanno

In una settimana almeno tre intrusioni hanno mostrato i problemi del settore

ALBERTO GHIARA

GENOVA. Nell'ultima settimana il problema della cybersicurezza nel mondo dello shipping è emerso in maniera consistente. A essere stati colpiti sono soggetti diversi, da una grande compagnia portaccontainer come Cgma-Cgm a una piccola società di cabotaggio come Red Funnel, fino al massimo organismo regolatore mondiale del settore marittimo, l'International Maritime Organization (Imo) delle Nazioni Unite. Proprio l'Imo è molto attiva sul fronte della sicurezza informatica e lavora costantemente per fornire agli operatori linee guida su come comportarsi per proteggere la propria attività imprenditoriale dagli attacchi di malintenzionati.

A partire dal primo gennaio 2021, l'Imo intende mettere nel mirino questo problema con una serie di audizioni sui sistemi di gestione della sicurezza a bordo e sul modo in cui vengono affrontati i rischi informatici connessi. Nel frattempo ha emanato una serie di linee guida con indicazioni sui comportamenti da tenere.

Di sicurezza informatica si è parlato recentemente a un convegno della Naples shipping week. Francesco Tozzi, esperto di sicurezza della società C3I, ha sottolineato come uno dei problemi principali siano le comunicazioni con soggetti terzi all'azienda, come fornitori

di beni e servizi, che possono aprire breccie nei sistemi aziendali. E ha ricordato il primo grande caso di questo tipo che ha riguardato lo shipping, quando nel 2017 vennero temporaneamente messi fuori uso i computer della compagnia Maersk. In quel caso, ha ricordato Tozzi, a fare da cavallo di Troia fu un fornitore di servizi finanziari che stava lavorando per la compagnia.

Degli attacchi avvenuti negli ultimi giorni, quello che ha destato maggiore preoccupazione è avvenuto al si-

stema della Cma-Cgm, per motivi di sicurezza e riservatezza non sono stati forniti dettagli sull'attacco, ma gli operatori che sono soliti interfacciarsi con i sistemi della compagnia hanno segnalato la presenza di problemi per parecchi giorni. La causa è stata identificata in un malware noto come Ragnar Locker. Si tratta di un virus del tipo ransomware, che rende inaccessibili tutti i dati registrati sul computer. Per liberare i dati, i criminali promettono l'invio di un codice in cambio del pagamento di un riscatto. Ma non sempre il pagamento del riscatto porta alla risoluzione del proble-

ma, per cui di solito viene sconsigliato il pagamento. Nel caso di compagnie grandi come Cma-Cgm, è possibile che vengano messi in atto sistemi di ridondanza che permettono di riprendere

l'attività, ma per il momento non sono stati forniti particolari in questo senso.

Negli stessi giorni, anche la compagnia di traghetti Red Funnel ha dovuto confrontarsi con lo stesso tipo di problema. L'amministratrice delegata Fran Collins ha detto che il problema sembrava essere «un attacco malevolo mirato a danneggiare la nostra operatività e a portare i nostri sistemi in tilt».

La compagnia ha spiegato che il risultato è stato che le prenotazioni online e telefoniche e i sistemi di gestione delle partenze non potevano più funzionare. Collins ha detto che l'obiettivo dell'attacco non era il furto di dati. Nel caso di Cma-Cgm invece si è parlato anche di una possibile intrusione nei database.

L'Imo a sua volta ha dovuto subire un attacco che ha messo temporaneamente fuori uso il suo sito internet. Il problema è stato successivamente risolto.

Nelle scorse settimane, come riportato da "L'Avvisatore Marittimo" del 23 settem-

bre, la Maritime Transportation System - Information Sharing and Analysis Center (Mts-Isac) degli Stati Uniti ha rivelato che per la prima volta un rimorchiatore statunitense è stato vittima di un attacco di questo tipo, attraverso una e-mail malevola. La società di rimorchiamento ha avvertito Louisiana



► 7 ottobre 2020

InfraGard, un'agenzia che fa riferimento dal dipartimento di Giustizia americano, che a sua volta ha avvertito Mts-Isac. Il malware era stato inviato con un'email che risultava partita da un indirizzo ufficiale della stessa società di rimorchio.

©BY NC AND ALCUNI DIRITTI RISERVATI



Una portacontainer della compagnia Cma Cgm