Internacional

UPS se pone a la altura de Fedex en EEUU

UPS anuncia un plan para igualar a su rival Fedex con un aumento del 4,9 por ciento en los precios en Norte América en 2015. Fedex anunció la misma subida en septiembre

Ciberataques en la industria marítima

Los expertos aseguran que “la voluntad de actuar contra el negocio es real”, como lo demuestra la violación del sistema del puerto de Antwerp para el tráfico de drogas

▶ La industria marítima y portuaria debe tomar cartas en el asunto para combatir el cibercrimen a escala global, porque, según los expertos, la amenaza es real. Así lo demuestra la violación del sistema informático de seguimiento de la carga en el puerto de Antwerp por criminales organizados para facilitar el tráfico de droga.

En el puerto de Antwerp ya hubo un ciberataque de unos criminales que violaron su sistema informático para el tráfico de droga.

IÑAKI CARRERA. Washington

Abogados de la firma estadounidense Blank Rome han advertido que la industria marítima y portuaria debe tomar cartas en el asunto para combatir el cibercrimen.

Según Steven Caponi y Kate B. Belmont, profesionales del prestigioso bufete con sede central en Washington, “la responsabilidad para defenderse activamente contra los riesgos de un ciberataque descansa directamente en los hombros de los armadores de los buques, las compañías marítimas, los operadores portuarios y otras empresas que también están envueltas en la industria”.

Los informes emitidos por la Oficina de Fiscalización de EEUU (GAO) y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) confirman que “esta industria es tan susceptible a los riesgos en ciberseguridad como las más vanguardistas firmas tecnológicas de Silicon Valley. Con capacidad para apropiarse de un barco, cerrar un puerto o una terminal, revelar documentos de precios altamente confidenciales o alterar manifiestos de carga o números de contenedores, incluso un ciberataque menor puede dar lugar a millones de dólares de negocio perdido y responsabilidad sobre terceros”, añadieron.

Mientras el origen de la amenaza varía, “desde las compañías rivales hasta organizaciones terroristas e incluso piratas o *hackers* que trabajan por su cuenta”, no hay duda de que “la voluntad de actuar contra la industria marítima es real”.

De hecho, “las principales compañías marítimas ya han empezado a sospechar que han sido víctimas de ataques deliberados de piratería informática. Es bien conocido que entre 2011 y 2013, hubo un ciberataque en el puerto de Antwerp orquestado por criminales organizados que violaron el sistema informático de la dársena, haciendo posible el tráfico de heroína y cocaína”, subrayaron Caponi y Belmont.

Desafortunadamente, la ciberseguridad de los mercantes y en los principales puertos “está de 10 a 20 años por detrás de los sistemas informáticos radicados en las oficinas y las industrias que compiten por todo el mundo”, añadieron.

Efecto dominó

Desde las perspectivas económica y de seguridad, la capacidad para interrumpir el flujo de mercancías marítimas en Europa o EEUU tendría un tremendo impacto negativo en las respectivas economías locales y también se dejaría sentir en todo el mundo. Dada la interconectividad de la industria marítima, el 90 por ciento del comercio exterior de la UE y el 45 por ciento del interior se realizan por barco, y la necesidad suprema de mantener el movimiento de los puertos con rapidez y eficiencia, “un ciberataque en sólo uno de los principales puertos de la UE o EEUU generaría un importante y negativo efecto dominó que afectaría a toda la industria”.

GAO y ENISA coinciden en que la parte más débil de la industria marítima es su confianza en las Tecnologías de la Información (TIC), que son cada vez más usadas en todos los niveles, desde la gestión de la carga hasta las comunicaciones que controlan el tráfico. Estos sistemas son comúnmente muy complejos y usan una diversidad de tecnologías.

Para mayor preocupación, “las TIC utilizadas por barcos, puertos y otras instalaciones están a menudo controladas remotamente desde lugares que se encuentran dentro y fuera del país. Además, algunos puertos han adoptado el uso de vehículos y grúas de patio automatizadas para facilitar el movimiento de los contenedores”, concluyeron.

La interferencia del GPS es un auténtico riesgo para la navegación

Según Steven Jones, director de la Asociación para la Seguridad en la Industria Marítima (SAMI, con base en Londres), la auténtica extensión de la amenaza es desconocida, pero “algunos expertos temen que los terroristas podrían usar mecanismos de gran potencia para interrumpir la recepción del GPS (Sistema de Posicionamiento Global) en los barcos ”.

Jones añadió que “los expertos también están reconociendo sin tapujos que la pésima defensa de los sistemas informáticos plantea un enorme riesgo para el *shipping*”. En opinión de David Last, un profesor emérito de la Universidad de Bangor en Reino Unido y toda una autoridad en la materia, “el GPS está tan integrado en el transporte, en las economías e industrias productoras de nuestras sociedades que el riesgo es alto”. Para Jones, la seguridad del GPS “no está sólo relacionada con la protección tecnológica. De hecho, hay ejemplos tales como la varada del crucero ‘Royal Majesty’ que deberían ser un aviso para todos los marinos de los peligros de depender de una fuente de información. Este barco encalló con más de 1.000 pasajeros abordo. El GPS había vuelto al modo ‘navegación por estima” o *dead reckoning* (DR) después de partirse una antena y no estaba dando una posición precisa”. “A pesar de estar en aguas costeras –continuó Jones-, los oficiales de guardia mostraron una confianza excesiva en la información que recibían de los elementos automatizados del puente de mando”.

Jones concluyó que “aunque este hecho no fue considerado como un acto intencionado y sospechoso, sí pone de manifiesto que un terrorista podía provocar deliberadamente un sabotaje sólo cortando un cable. La navegación y las maniobras de un barco son vulnerables, y deben adoptarse medidas para gestionar este problema de la seguridad”.