BOLETÍN CHUBB MARINE-LOGICA "RIESGO CIBERNÉTICO EN EL TRANSPORTE MARÍTIMO"

Número 25

"RIESGO CIBERNÉTICO EN EL TRANSPORTE MARÍTIMO"

Mientras que la automatización podría conducir a un ahorro significativo, inicialmente los equipos de control nunca tuvieron la intención de ser conectados a Internet lo que actualmente podría dejar a los buques vulnerables al terrorismo, la piratería y la destrucción.

La industria marítima, presenta rezagos, para hacer frente a los riesgos cibernéticos, Según los informes, existen debilidades significativas en la seguridad cibernética de tecnologías esenciales para la navegación marítima. Los GPS (Sistema de Posicionamiento Global), AIS (Sistema de Identificación Automática), y ECDIS (Sistema de Información y Visualización de Mapas Electrónicos) son herramientas clave para la navegación, y todas podrían estar vulnerables a un ataque.

La Organización Marítima Internacional (OMI) es el organismo de las Naciones Unidas a cargo de la protección y seguridad del transporte marítimo. Desde el 2004 requirió la instalación de AIS en todos los barcos de pasajeros, en cargueros con un Arqueo Bruto (GT) superior a 500 GT, y en buques de comercio internacional con más de 300 GT. El AIS ha llegado a suplir el radar como instrumento de navegación en los barcos, y también es parte integral de los sistemas de separación de tráfico marítimo utilizados por organizaciones asignadas a la seguridad en alta mar. Dado que el AIS carece de un mecanismo para cifrar o autentificar señales, es considerado un blanco fácil para los ataques cibernéticos, y en el 2013 la empresa de seguridad cibernética Trend Micro2 lo comprobó. Demostró la vulnerabilidad del AIS al impedir que un buque diera información sobre sus movimientos, al hacer aparecer buques o estructuras "fantasma". Asimismo, creó emergencia simuladas, e hizo creer a otros usuarios del AIS que un buque estaba en una ubicación falsa.

Las compañías marítimas se enfrentan a amenazas cibernéticas significativas ya que en la actualidad los buques están adaptando su equipo de navegación, operativo y otros a las nuevas tecnologías del mundo digital.

elementos: Información, Tecnología y Personas. La **información** se refiere a los datos que sustentan las operaciones marítimas, sus usos y las formas en que la información puede ser manipulada en la edad moderna. **Tecnología** encapsula los sistemas informáticos, tanto de hardware como de software y sistemas operativos, incluyendo buques y puertos. La tecnología es fundamental en la navegación por el entorno marítimo, pero también es tanto física como digitalmente vulnerable. Las **Personas** son parte de sistemas complejos. Los tres elementos interactúan entre sí de dos maneras: Creativas y destructivas. En cada interacción de humano y máquina existe la posibilidad de error, la manipulación, la coerción o la sedición. Por ejemplo se puede estar conectado físicamente al mar u otro cuerpo de agua a través de la tecnología digital desde instalaciones en tierra, en las que se actúa como si estuvieran a bordo plataformas o buques. En el caso de las personas, éstas pueden estar conectadas a uno o más grupos sociales con base en tierra y tener comunicación en tiempo real, de manera mucho más amplia de lo que habían sido previamente capaz de hacer.

Ante éste tipo de riesgo lo lógico es calcular la probabilidad de que ocurra un incidente que cause pérdidas y valorar la máxima exposición analizando diferente escenarios para tomar decisiones adecuadas para el manejo del riesgo.

Es importante señalar que la gestión de riesgos tradicional no es aplicable para el tipo de amenazas cibernéticas. El enfoque en éste caso es generar estrategias y tecnología para seguridad en la información electrónica.

Actualmente en la industria marítima existe una nueva

Hasta hace algunos años, la mayoría de los ataques cibernéticos eran con la finalidad de obtener datos personales o financieros delicados. Hoy en día, el tipo de amenaza ha cambiando, y compañías de todos los sectores han comenzado a sufrir ataques sofisticados que tratan de infligir daños a la propiedad y a las operaciones, con el fin de apoderarse de sistemas de control industrial.

Los nuevos sistemas usan datos de terminales remotas para controlar ciertos procesos automáticamente o a través de un operador, y están diseñados para excluir al resto del mundo. Hackers talentosos han demostrado que son capaces de penetrar los sistemas usados por la industria marítima, lo cual podría acarrear consecuencias desastrosas.

Los sistemas de navegación y propulsión de los buques, los sistemas de manejo de carga y rastreo de contenedores en los puertos y a bordo de los barcos, y los inventarios y procesos automatizados en los astilleros, están controlados con un software necesario para agilizar las operaciones. Los ataques cibernéticos también pueden ser por razones delictivas como secuestrar, desviar o robar mercancía. (*Como se vió en Amberes entre 2011 y 2013 en el que piratas cibernéticos que operaban junto con una organización de narcotraficantes infiltraron el sistema de rastreo del puerto de Antwerp (Bélgica) para identificar los buques que transportaban cargamentos de drogas y fármacos. La organización logró desviar con éxitos los contenedores del puerto para retirar las drogas de estos y luego cubrir sus pasos. Esta operación fue realizada frecuentemente durante dos años, hasta que una operación en conjunto de la policía belga y holandesa logró detenerla*. *FUENTE: http://www.bbc.com/news/worldeurope-24539417*) Los eventos de los últimos cuatro años sugieren que este tipo de sistemas están cada vez más expuestos a ese tipo de ataques. tendencia de promover buques drones (No tripulados) los

Las amenazas cibernéticas se extienden a los puertos, cuales tienen un gran riesgo de “Piratería Cibernética” en también. Las "Medidas básicas de seguridad cibernética la que hackers podrían apoderarse de los mismos así no se están practicando en estas instalaciones”, dijo el como utilizarlos para actos de terrorismo y/o guerra

Instituto Brookings con sede en Washington, en un cibernética. Por ejemplo, si inhabilitaran un buque en informe de julio de 2013. medio de algún canal marítimo de alto tráfico, podría generar repercursiones económicas. Para comprender las vulnerabilidades antes mencionadas a continuación se explica cómo interactúan las operaciones cibernéticas en el ámbito marítimo lo cual puede ser discutido en términos de tres

MÉXICO
DIRECCIÓN DE TRANSPORTES
Omar Mendoza Lizaola (omar.mendoza@chubb.com)
Alfredo Martínez (alfredo.martínez@chubb.com)
Asdrúbal Sánchez (asanchez@logicapty.com) editó

Elaboró: Alfredo Martínez