Grúas y Transportes

Sitio de WordPress.com

Riesgos de manejar las terminales automatizadas desde el extranjero

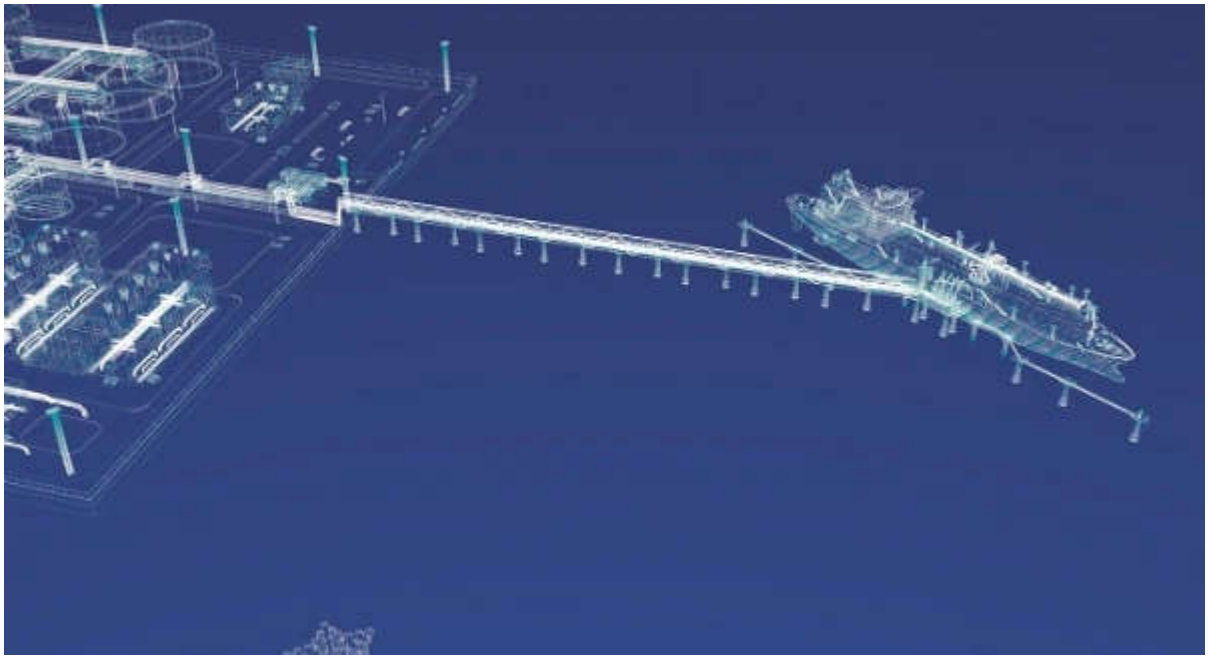
22/02/2020 Deja un comentario

Riesgos de manejar las terminales automatizadas desde el extranjero

.

Expertos cuestionan los riesgos de manejar las operaciones automatizadas de las terminales desde el extranjero

Publicado el Jueves, 23 de enero de 2020.
Por Zoe Reynolds, corresponsal.
Traducido por Gustavo Zamora (https://ar.linkedin.com/in/gustavozamora)*, Buenos Aires (Argentina) para gruasytransportes.
.



.
Esquema del puerto con representación 3D. Crédito: Getty Images
Se prevé que aumente la nueva tendencia de controlar los puertos automatizados en forma remota. El parlamento australiano y los expertos en ciberseguridad cuestionan los riesgos de manejar las operaciones automatizadas de las terminales desde el extranjero.
Todo estaba parado en la terminal de contenedores de Webb Dock, Melbourne, el 5 de junio de 2019. Las grúas robótizadas blancas que se deslizan con gracia entre los camiones y las montañas de contenedores, permanecian inmóviles. Las grúas pórtico STS gigantes de barco a tierra que mueven los contenedores dentro y fuera de los barcos, estaban sin vida. La primera terminal de contenedores totalmente automática de Australia se paralizó temporalmente.
“La Terminal Internacional de Contenedores de Victoria [VICT] experimentó una interrupción esta mañana, que afectó tanto a las operaciones en tierra como a los buques. La razón de la interrupción se debió a un error de comunicación del sistema entre el sistema de programación de trabajos y las grúas de VICT”, anunció la compañía a sus clientes en un aviso distribuido por Freight and Trade Alliance ese día.
Ya sea una falla en la red informática o algo más siniestro que interrumpe la conexión a la Nube que recorre 6.339 km entre Manila y Melbourne esa mañana de invierno, el portavoz de la compañía declinó hacer comentarios. Sin embargo, el incidente destaca los posibles problemas de seguridad y las fallas técnicas que podrían ocurrir en puertos controlados de forma remota.
VICT, una subsidiaria de propiedad total de International Container Terminal Services, Inc (ICTSI) de Filipinas, está ampliando los límites de las operaciones portuarias que funcionan a control remoto. Sus trabajadores observan pantallas de computadora en las oficinas de la subsidiaria ICTSI, Australian Pacific Business Services (APBS) Inc en Manila, quienes programan los movimientos de los contenedores como piezas virtuales de Lego en los muelles de Melbourne.
Justo subiendo por la carretera desde los muelles en Five E-Com Center, Harbor Drive, Pasay, el “equipo de Manila”, como los conoce la gerencia de VICT, cubren las operaciones de control de equipos desde el gate con seguridad automática hasta la flota de grúas automáticas de apilamiento de plazoleta/patio de Melbourne, utilizando los últimos sistemas operativos digitales de terminales y con alimentación de video a través de la nube (satélite e internet). Los trabajadores en Manila se comunican con los trabajadores portuarios y con los camioneros australianos día y noche.
ICTSI, que opera 32 terminales en 19 países, lanzó su subsidiaria de servicios compartidos APBS en diciembre de 2015. Esta información estaba publicada en el sitio web de la compañía, hasta hace poco, y

fue cubierta por la prensa de Manila. La compañía describió el negocio como una operación de outsourcing para sus subsidiarias y afiliadas en la región de Asia-Pacífico y otros clientes. Ganó el contrato como el tercer operador de Melbourne en 2014. Con el aumento de los puertos automatizados, la inteligencia artificial y la "tele-robótica" controlada de forma remota capaz de pilotear máquinas desde lejos, es probable que otros operadores portuarios hagan lo mismo.

Es el equipo de ICTSI en Manila con quien habla el conductor del camión australiano después de colocar la parte trasera del camión bajo un haz de luz y retrocede hacia la casilla para dejar que la grúa robot levante o baje la carga. Las tareas del Control de equipos de Melbourne (EC) realizados ahora en Manila también cubren la planificación del patio/plazoleta, el trabajo administrativo, la mesa de ayuda, la planificación de las embarcaciones y el "trabajo de EC de overflow del lado tierra" para las grúas de patio/plazoleta, según los trabajadores de la terminal.

Entonces, ¿hasta dónde puede llegar el control remoto de las terminales de contenedores y cuáles son los riesgos? ¿Podrían las operaciones globales de la terminal de contenedores de una compañía en todo el mundo ser operadas de forma remota desde una torre de control central? ¿Podría China monitorear y controlar sus 40-50 terminales salpicadas a lo largo de su nueva Ruta de la Seda marítima que abarca Medio Oriente, Europa, América del Sur, África, Asia y Australia desde una torre de operaciones central en Beijing o en Hong Kong?

Una compañía líder en sistemas operativos de terminales está anunciando su software, permitiendo a los estibadores "ejecutar sus operaciones, desde una sola terminal a múltiples terminales en múltiples ubicaciones geográficas, todo en una sola instancia". Una terminal en Noruega ha comenzado a manejar los trabajos de sus equipos moviles desde Turquía, según la Federación Internacional de Trabajadores del Transporte (ITF).

En Melbourne, los trabajadores aún operan las grúas de control remoto de barco a tierra desde el interior de la terminal, a pesar de las señales previas de que también se trasladaría esa función al extranjero. Según Fredrik Johanson, gerente general de marketing y ventas de ABB Crane Systems, las conexiones de satélite e internet sufren retrasos en el tiempo, lo que dificulta el manejo desde el extranjero de las operaciones críticas. "Pero con la introducción de la inteligencia artificial, eso también cambiará y no habrá límite en cuanto a cómo pueden ser controladas a distancia las operaciones remotas ", imaginó, hablando en el 2015.

Si bien se han producido avances tecnológicos desde que Johanson hizo esos comentarios, el manejo desde el extranjero de las operaciones portuarias ha hecho sonar las alarmas entre los expertos en seguridad cibernética. También se han planteado preguntas en el parlamento australiano.

El riesgo cibernético

En declaraciones al comité de estimaciones del Senado el 21 de octubre, el senador Kimberley Kitching interrogó al subsecretario de Asuntos Interiores, seguridad y resiliencia, Paul Grigson, sobre si los gates de entrada/salida de seguridad, las grúas automáticas de patio/plazoleta y los sistemas operativos de las terminales se estaban desviando a Manila. También preguntó si los trabajadores filipinos tenían que someterse a alguna de las verificaciones de seguridad como lo hacen los trabajadores australianos. Grigson dijo que no lo sabía y respondió todas las preguntas.

Kitching también planteó la cuestión de las infracciones en el gate de seguridad en VICT. "Si usted es un conductor de camión, se presenta en el puerto de Melbourne y toda su interacción sería [con] alguien que esté en Manila, Filipinas, ¿correcto? Supongo que la pregunta es, sin una verificación física, ¿como se evita que varios conductores usen la misma tarjeta? Teóricamente, ¿podría alguien en Manila abrir remotamente un gate de seguridad sin una tarjeta de seguridad? ", preguntó. Kitching también preguntó si alguien que no había tenido que pasar por ningún nivel de control de seguridad podría ingresar a un importante puerto australiano, o si Asuntos del Interior había realizado una auditoría del puerto de Melbourne.

"Hacemos las auditorías, pero no sé si hemos hecho esa auditoría alli", respondió Grigson, comprometiéndose a averiguarlo. Tres expertos australianos en ciberseguridad contactados por SAS han

pedido una mayor supervisión gubernamental y auditorías portuarias. Lani Refiti, socio de Cyber Risk Advisory Practice, Deloitte Australia, ha asesorado a algunas de las operaciones mineras y a los proveedores portuarios más grandes del mundo sobre automatización y seguridad cibernética.

Los riesgos cibernéticos aumentan en los puertos a medida que se vuelven más automatizados y el control de las operaciones se traslada al extranjero debido a que aumenta la amenaza del riesgo sobre la cadena de suministro y el riesgo de terceros, dijo Refiti. El puerto de Melbourne está cubierto por la Ley de Infraestructura Crítica, que requiere propiedad registrada e información operativa, agregó. "Es necesario que se realice una garantía / validación y una gobernanza continua de la seguridad cibernética. Los puertos deberían adherirse al marco de las mejores prácticas de la industria ", dijo Refiti. Esto es importante cuando se considera que el trasladar el control de las operaciones al extranjero está ahora muy difundido a nivel mundial, según Refiti. "Creo que es hacia donde se dirige el mundo", dijo. "Puede ser más eficiente y rentable. Es solo que el perfil de riesgo es más alto ".

Refiti recomienda a los gobiernos que contraten a un tercero para probar los controles de seguridad, que examinen las obligaciones contractuales de la empresa con terceros y averigüen exactamente qué está sucediendo y dónde podrían estar los riesgos. Además, los inquilinos individuales deberían informar al puerto si trasladan controles al exterior, dijo. "No se debería hacer nada de esta magnitud sin que el puerto lo sepa", agregó.

Según la Ley de Seguridad de Infraestructura Crítica de 2018, los puertos deben reportar información sobre quién está operando un activo o parte de un activo al Registro de Activos de Infraestructura Crítica, dijo el Departamento de Asuntos Internos de Australia a SAS. Cuando se le preguntó sobre la sabiduría de las corporaciones multinacionales que tienen el control y la gestión de la infraestructura crítica de una nación en el extranjero, Refiti dijo que sería escandaloso si los gobiernos miraran hacia otro lado.

ICTSI / VICT declinó hacer comentarios sobre este tema cuando fue contactado por el escritor en varias ocasiones. Sin embargo, está haciendo esfuerzos para mejorar la seguridad del puerto automatizado. El 19 de noviembre, la compañía anunció actualizaciones a sus protecciones de seguridad cibernética; estaba implementando la tecnología BlackBerry Cylance en su red global.

"Las economías nunca duermen, y tampoco los hackers", dijo Brian Hibbert, director de información de ICTSI. "La seguridad cibernética es nuestra prioridad en ICTSI, y por eso necesitamos tecnología igualmente sofisticada impulsada por la inteligencia artificial como BlackBerry Cylance para proteger nuestros activos".

Los puertos están mejorando su juego para evitar la interrupción y los mayores costos que pueden resultar de un ataque cibernético. Evan Davidson, vicepresidente de ventas de BlackBerry Cylance APAC, citó el Centro de Estudios de Riesgo de Cambridge / Lloyds estima que "un ataque cibernético a los puertos asiáticos a través de navieras podría costar hasta USD110 mil millones, la mitad de la pérdida global total por catástrofes naturales en 2018 ". Reconoció que ICTSI necesitaba aumentar su madurez cibernética. "Ellos [ICTSI] ejecutaban tres versiones de software cibernético y no tenían la intervención crítica que necesitaban", dijo a SAS.

Davidson declinó comentar si ICTSI había sufrido ataques cibernéticos en el pasado. Sin embargo, afirmó que CylancePROTECT es un software que utiliza algoritmos de inteligencia artificial y aprendizaje automático para "detectar, prevenir y contener malware existente y nuevo que evitará amenazas", dijo.

"Ninguna compañía puede afirmar que sus productos de seguridad pueden proteger al 100% de todas las amenazas de seguridad de la información. El uso de soluciones de seguridad cibernética de IA tampoco es una bala de plata que nunca fallará, sin embargo, los evaluadores independientes han demostrado que es 99,1% efectivo para predecir y prevenir ataques cibernéticos en el punto final ", dijo, citando estudios que muestran el software tiene una ventaja predictiva de hasta 33 meses.

"BlackBerry Cylance es una herramienta de seguridad cibernética y una buena opción, pero no puede ser una garantia contra todos los ataques", dijo Refiti, afirmando que la mayoría de las infracciones de

seguridad se debían a errores humanos e interacción, como herramientas de seguridad mal configuradas o que están mal utilizadas.

"La IA [seguridad cibernética] no funcionará por sí sola", explicó. "Puede convertirse en un peligro porque las personas tienen una falsa sensación de seguridad. Una tecnología como esta ayuda, pero es inútil si no se la usa correctamente ", dijo. Por ejemplo, no detendría un ataque de denegación de servicio: un ataque cibernético destinado a apagar una máquina o red y hacerla inaccesible para los usuarios previstos. "Si niega el acceso de un proveedor de servicios externo a los sistemas informáticos del puerto para monitorear y administrar, entonces probablemente sea un riesgo mayor que robar datos", dijo.

Al igual que Refiti, el estratega australiano de la Fuerza Aérea John Blackburn RAAF (retirado), ex jefe de política estratégica de defensa, describió el manejo de la infraestructura crítica desde el extranjero como una carga con peligro. "¿Las suposiciones se hacen a través de la lente de un negocio internacional, y no de la lente de la seguridad nacional?", preguntó. "Necesitamos un enfoque basado en escenarios: el tipo de trabajo que hice con los militares. ¿Hay algún adversario que quiera derribar el sistema?

Blackburn preguntó si el gobierno australiano había completado el análisis de riesgos. "Si algo se automatiza, se controla desde el extranjero, brindando servicios a Dios sabe quién, cuáles son los riesgos", preguntó. Si bien reconoció los innumerables beneficios de la automatización, hizo hincapié en que no debería dejarse en manos de los intereses comerciales, y pronosticó que es una cuestión de política que "volverá a mordernos eventualmente",

Blackburn también advirtió sobre el riesgo de que gobiernos extranjeros recopilen inteligencia a través de la propiedad o el control de activos nacionales y solicitó una auditoría de la infraestructura crítica. El profesor asociado Carsten Rudolph de seguridad cibernética, Escuela de Tecnología de la Información, Universidad de Monash, fue más allá; Los sistemas de control remoto podrían crear objetivos para la guerra, advirtió.

"Los sensores y la señal de la cámara se pueden piratear y manipular para que la vista que se obtiene no muestre deliberadamente lo que está sucediendo", dijo, señalando el ataque cibernético de 2008 que incendió un oleoducto en Turquía. Rudolph enfatizó que ningún control de seguridad único, ni siquiera herramientas avanzadas de seguridad cibernética como CylanceProtect, podría garantizar la seguridad. "Se requiere una visión de todo el sistema", dijo. "Somos bastante malos en la construcción de sistemas seguros. El análisis de riesgos debe realizarse antes de establecer los sistemas. Desde el punto de vista de la seguridad, debemos evaluar los riesgos de trasladar empleos a países más baratos".

No solo los expertos en ciberseguridad han expresado sus preocupaciones, sino también los expertos de la industria. Peter van Duyn es un experto en logística marítima del Instituto de Cadena de Suministro y Logística, Universidad de Deakin, director de la Asociación Internacional de Coordinación de Manejo de Carga y ex gerente de las terminales Patrick de Australia, que fue pionera en la automatización de puertos en Australia. "Gran parte del trabajo se puede hacer desde una torre de control en cualquier lugar", dijo. "Pero aún necesitamos personas en el terreno, incluso con una terminal automatizada, para que puedan trabajar juntas, especialmente si hay algún problema".

El impacto en el comercio naviero

"La globalización está sucediendo y sin dudas continuará", dijo van Duyn. "Pero Maersk es una advertencia. Si todo el país se detiene debido a algo como esto, podría ser una llamada de atención".

En junio de 2017, el imperio global naviero y de puertos de AP Moller Maersk se convirtió en un daño colateral en la guerra cibernética de Rusia contra Ucrania. Solo se necesitó que un ejecutivo de finanzas en la terminal de Odessa de la compañía en el Mar Negro cargara un popular programa de software de contabilidad en una sola computadora para borrar todos los datos de la red global de la compañía. Las terminales que abarcaban 76 puertos en todo el mundo estaban paralizadas, y fueron las terminales automatizadas las más afectadas. Tal fue la magnitud de la violación del malware – llamado notpetya- , que incluso se han escrito libros al respecto.

El escritor Andy Greenberg describe terminales de contenedores en coma desde Long Beach, Los Ángeles, hasta Rotterdam, Europa, en su libro Sandworm. Los sistemas informáticos colapsaron, las grúas del muelle se congelaron, los gates se cerraron, y decenas de miles de camiones están haciendo cola, 800 barcos yacen muertos en el agua. El comercio naviero se vio afectado cuando los manifiestos y otros datos digitales desaparecieron. Los buques portacontenedores de Maersk, que representan cerca de una quinta parte del comercio mundial, se balanceaban en el mar sin poder ingresar a los puertos.
La compañía tuvo mucha suerte de poder reiniciar todo después de solo una o dos semanas. La ciudad de Ghana, en África, sufrió un corte de energía eléctrica que desconectó las computadoras de la terminal local de AP Moller Maersk de la red global, el día de la violación de seguridad, escribió Greenberg. El único controlador de dominio sobreviviente fue trasladado y entregado personalmente a un equipo de alrededor de 200 expertos de TI de Deloitte que trabajaban las 24 horas con 400 empleados de Maersk en la sede de Maidenhead en el Reino Unido.
"Después del primer día, las operaciones portuarias de Maersk habían recuperado la capacidad de leer los archivos de inventario de los barcos, por lo que los operadores ya no estaban cegados al contenido de los enormes, buques de 18.000 [teus] que llegaban a sus puertos", escribió Greenberg.
Los ataques cibernéticos más recientes incluyeron Long Beach y San Diego, Estados Unidos; el puerto de Barcelona, España; y el constructor naval de la defensa de Australia, Austal en Perth. "El aumento de la automatización y la disminución de la intervención manual en la industria marítima proporciona un terreno fértil para las violaciones de seguridad", escribió la Dra. Indra Vonck, experta portuaria, de Deloitte, para la Organización de Puertos Bálticos en 2017. "La seguridad cibernética en los barcos y en los puertos ahora es de suma importancia, ya que el impacto económico en la industria naviera y en las operaciones portuarias es enorme", advirtió.
El Puerto de Melbourne fue auditado el 5 de diciembre de 2017 y será auditado nuevamente este año financiero, según el Departamento de Asuntos Interiores de Australia. El puerto de Melbourne y VICT operan de acuerdo con los planes de seguridad marítima aprobados por el Departamento del Interior en virtud de la Ley de Instalaciones Marítimas y de Transporte Marítimo de 2003. Debido a razones de privacidad y seguridad, los resultados de la auditoría y el contenido de los planes de seguridad no pueden divulgarse públicamente .

.

Safety at Sea

.

Read it in English at:

.

https://safetyatsea.net/news/ (https://safetyatsea.net/news/2020/experts-question-risks-of-offshoring-automated-terminal-operations-in-australia/)2020/experts-question-risks- (https://safetyatsea.net/news/2020/experts-question-risks-of-offshoring-automated-terminal-operations-in-australia/)of-offshoring-automated- (https://safetyatsea.net/news/2020/experts-question-risks-of-offshoring-automated-terminal-operations-in-australia/)terminal-operations-in- (https://safetyatsea.net/news/2020/experts-question-risks-of-offshoring-automated-terminal-operations-in-australia/)australia/ (https://safetyatsea.net/news/2020/experts-question-risks-of-offshoring-automated-terminal-operations-in-australia/)

Read it in English at:

.

https://felixstowedocker. (https://felixstowedocker.blogspot.com/2020/01/experts-question-risks-of-offshoring.html)blogspot.com/2020/01/experts- (https://felixstowedocker.blogspot.com/2020/01/experts-

question-risks-of-offshoring.html)question-risks-of-offshoring. (https://felixstowedocker.blogspot.com/2020/01/experts-question-risks-of-offshoring.html)html (https://felixstowedocker.blogspot.com/2020/01/experts-question-risks-of-offshoring.html)
==========

Descargue el archivo pdf de este artículo en:

Fuentes – Sources:

Ver arriba en cada foto y articulo.

(*)Gustavo Zamora es un especialista en equipo de elevación y manejo de cargas. Vive y trabaja en Buenos Aires (Argentina)

Tags:

Experts question risks of offshoring automated terminal operations (gz39),

Si quiere colocar este post en su propio sitio, puede hacerlo sin inconvenientes,

siempre y cuando no lo modifique y cite como fuente a https://gruasytransportes.wordpress.com (https://gruasytransportes.wordpress.com/)

Recuerde suscribirse a nuestro blog vía RSS o Email.

==========

Otros posts relacionados:

– Grúas en puertos automatizados. (https://gruasytransportes.wordpress.com/tag/gruas-en-puertos-automatizados/)

.

==========

15940
==========

Etiquetado:correccion de manuales traducidos (https://gruasytransportes.wordpress.com/tag/correccion-de-manuales-traducidos/), felixstowedocker (https://gruasytransportes.wordpress.com/tag/felixstowedocker/), Grúas en puertos automatizados (https://gruasytransportes.wordpress.com/tag/gruas-en-puertos-automatizados/), Grua (https://gruasytransportes.wordpress.com/tag/grua/), Gustavo Zamora (https://gruasytransportes.wordpress.com/tag/gustavo-zamora/), ICTSI (https://gruasytransportes.wordpress.com/tag/ictsi/), notpetya (https://gruasytransportes.wordpress.com/tag/notpetya/), traduccion de manuales (https://gruasytransportes.wordpress.com/tag/traduccion-de-manuales/), traduccion tecnica (https://gruasytransportes.wordpress.com/tag/traduccion-tecnica/), traductor (https://gruasytransportes.wordpress.com/tag/traductor/), VICT (https://gruasytransportes.wordpress.com/tag/vict/)