[notasdeprensa.jpg](http://www.notasdeprensa.es)Publicado en España el 17/12/2019

# [NTT revela cuatro pasos para garantizar la seguridad cibernética en barcos y puertos](http://www.notasdeprensa.es)

## Piratas digitales, una nueva amenaza para la industria del transporte marítimo

Los piratas informáticos atacan cada vez más los barcos y puertos. Debido al aumento del uso de la tecnología de gestión de datos y las redes de TO (Tecnología Operacional) y TI (Tecnología de la Información), estas suponen un objetivo de la misma magnitud que las compañías tradicionales en tierra. La División de Seguridad de NTT Ltd., uno de los principales proveedores de servicios tecnológicos del mundo, aconseja a las compañías navieras que sigan cuatro pasos para detener la piratería digital. Ya se trate de los sistemas de navegación en el puente de mando, el mantenimiento de los enormes motores o la documentación de los contenedores individuales, cada vez más la tecnología de datos está encontrando su sitio a bordo. Para las compañías navieras, esto ofrece numerosas ventajas: los sensores y transmisores pueden, por ejemplo, enviar información a tierra sobre el estado de la tecnología. Si se informa de un mal funcionamiento, los empleados pueden tener preparado los repuestos necesarios a su llegada al siguiente puerto. Esto reduce considerablemente los costes en los que normalmente se incurriría por el desplazamiento de técnicos y piezas. Para lograr tener información en tiempo real de todos los sistemas, como motores, timones, hélices y lastre, es esencial la conexión en red entre los sistemas TO y TI. Sin embargo, esta interconexión de las dos redes elimina la separación estanca que solían existir entre los dos sistemas y abre nuevas puertas de entrada para los ciberdelincuentes. Si los barcos se convierten en víctimas de un ataque de piratas informáticos, podría dar lugar a barcos incontrolados en alta mar o en áreas portuarias e incluso provocar colisiones. Dichos escenarios de terror son particularmente temidos en la operación de naves no tripuladas, las cuales se esperan en un futuro próximo. Otros escenarios son, por ejemplo, los ciberataques en grandes puertos que cierran terminales o manipulan cargas de contenedores y datos confidenciales. Dichos ataques pueden provocar daños considerables debido a interrupciones en las operaciones o pérdida de reputación. Para mitigar el riesgo de ciberataques, las empresas deben simular posibles escenarios e identificar medidas apropiadas para mitigar el riesgo: - El primer paso es la piratería ética. Las pruebas de seguridad con comprobadores de penetración profesionales, que conocen bien la industria marítima, ayudan a encontrar brechas de seguridad en todas las áreas, desde sistemas de acceso hasta redes y sistemas operativos, y luego cerrarlas con las medidas adecuadas. Basándonos en la experiencia de NTT, los sistemas de control marítimo como la navegación o el control de bombas de los depósitos de lastre son siempre un objetivo fácil. - El segundo paso es monitorizar las redes del entorno de TI y TO. Esto se puede hacer con sensores que pasivamente "monitorizan" el tráfico de red, lo analizan y buscan desviaciones del "comportamiento normal". Estas desviaciones se reportan automáticamente. - El tercer paso es procesar todas las alarmas continuamente. Si el sistema de monitorización informa de errores, los expertos deben verificar de inmediato si se trata de un incidente grave o de tráfico normal. Aquí, por supuesto, hay restricciones en el análisis central por conexiones satelitales de los barcos en alta mar. - El cuarto paso es un programa integral de gestión de emergencias y respuesta a incidentes. En caso de una advertencia grave, se deben tomar medidas inmediatas para evitar el éxito de un ataque a los datos. Esto requiere la experiencia necesaria para evitar daños que puedan poner en peligro a las personas, los materiales, las finanzas y la reputación. "Los riesgos cibernéticos son una nueva amenaza para la industria del transporte marítimo, que está altamente interconectada y depende cada vez más de la automatización en sus operaciones. Un ataque de piratas informáticos a la tecnología a bordo, en particular a los sistemas de navegación electrónica, podría provocar una pérdida total e incluso afectar a varios barcos de una compañía naviera. Por lo tanto, las compañías deben simular posibles escenarios e identificar medidas adecuadas para reducir el riesgo", explica Christian Koch, Director de GRC (Gobernabilidad, Riesgo y Cumplimiento) e IoT / TO en la División de Seguridad de NTT Ltd. "Aunque el problema de seguridad para los sistemas de TI y TO en red en los barcos es aún tan reciente que las regulaciones legales han sido hasta ahora una excepción, todavía es una cuestión de futuro. Sin embargo, hay algunos estándares como NIS, MTSA3 y VIQ7 que contienen las pautas correspondientes. Las empresas que siguen estos cuatro pasos anteriormente mencionados están en vías de cumplir con estos estándares ".

**Datos de contacto:**

Juan Maldonado

+34 619 743 694

Nota de prensa publicada en: [https://www.notasdeprensa.es/ntt-revela-cuatro-pasos-para-garantizar-la](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorias: Telecomunicaciones Nautica E-Commerce Ciberseguridad Dispositivos móviles Sector Marítimo

[notasdeprensa.jpg](http://www.notasdeprensa.es)

[**http://www.notasdeprensa.es**](http://www.notasdeprensa.es)