EL PUERTO DE VALENCIA A LA VANGUARDIA DE LA CIBER-SEGURIDAD A TRAVÉS DEL PROYECTO MEDUSA

Valencia, 6 de mayo de 2016.- Esta mañana se ha celebrado, en las instalaciones de la Autoridad Portuaria de Valencia (APV), la conferencia internacional **"Cyber-security in the Supply Chain: New approaches and challenges**", organizada en el marco del proyecto MEDUSA, cofinanciado por la DG HOME - Comisión Europea - a través del Programa de Prevención, preparación y gestión de las consecuencias del terrorismo y otros riesgos relacionados con la seguridad.

La jornada, organizada por la APV, la Fundación Valenciaport y Feports, que participan en el proyecto como miembros de la Agrupación Europea de Interés Económico - EUROPHAR, ha sido inaugurada por el director de Seguridad y Medio Ambiente de la APV, Federico Torres y por el director general de la Fundación Valenciaport, Vicente del Río. Federico Torres durante su intervención ha destacado la participación de la APV en distintos proyectos de seguridad así como la puesta en marcha de iniciativas pioneras como el CSI (Container Security Management), MEGAPORTS o la certificación de la ISO 28000. Por su parte, Vicente del Río ha señalado que la Fundación Valenciaport, como miembro de EUROPHAR, es consciente de la importancia que tiene la seguridad, tanto física como cibernética, dentro de la cadena logística portuaria, para garantizar la eficiencia y la competitividad de las economías nacionales. Y es por esto, que se involucra en proyectos de cooperación de ámbito europeo, como el proyecto MEDUSA.

A continuación, Christos Douligeris, profesor de la Universidad del Pireo, ha presentado los principales resultados del proyecto MEDUSA:

- Una herramienta orientada a evaluar los riesgos relacionados con las infraestructuras de la información y comunicación que interaccionan a lo largo de la cadena de suministro

- Una propuesta de medidas de prevención y de respuesta ante la detección de cualquier amenaza identificada en cualquier nodo de la cadena logística

- Una descripción de los escenarios tipo más relevantes con la finalidad de evaluar la herramienta, basados en el transporte de contenedores, vehículos y GNL.

La jornada ha continuado con las intervenciones de Fernando Seco, director consultor de S2 Grupo, que ha impartido una ponencia sobre la ciber-seguridad en la cadena de suministro y Rafael Pedrera, director de operaciones de la Oficina de Ciber-Coordinación del Centro Nacional Para las Infraestructuras Críticas (CNPIC) y Alfonso Ruiz, de la misma entidad, que han hablado sobre la protección de las infraestructuras portuarias críticas.

A continuación, Manuel Esteve, director del Laboratorio de Sistemas en Tiempo Real de la UPV, ha presentado un sistema de control y gestión de mando integrado con la aplicación de nuevas técnicas de visualización para mostrar el ambiente real y el ciberespacio.

Por su parte, Pablo Noval, director técnico de Saggas, ha descrito el flujo de la cadena de transporte del gas natural licuado detallando los distintos actores que participan en la cadena de suministro.

Los riesgos y desafíos de la cadena logística del transporte de contenedores han sido presentados por José Gisbert, Responsable de Tecnologías de la Información de MSC Terminal Valencia. Gisbert ha explicado las relaciones que mantiene una terminal de contenedores con los agentes externos de la cadena de suministro, las normativas a seguir para garantizar la seguridad, los principales riesgos y amenazas a los que se exponen y qué hacer para mitigarlos.

Durante la sesión de demostraciones, Spyros Papastergiou, del Centro de Investigación de la Universidad de Pireo, ha presentado el "MEDUSA Toolkit", una herramienta que ha sido diseñada y desarrollada en el marco del proyecto y que permite un análisis exhaustivo de riesgos y amenazas, tanto físicas como cibernéticas, teniendo en cuenta el "efecto cascada" de todo el proceso de transporte a través de la identificación de todos los flujos de intercambio de información entre los numerosos sistemas de comunicación existentes.

Por su parte, Stefan Schauer, del departamento de Seguridad y Protección digital del Instituto Tecnológico de Austria, ha presentado MITIGATE, un proyecto auspiciado por el programa H2020, cuyo objetivo es crear un sistema que permita avisar de cualquier riesgo cibernético, informando del nivel de importancia así como un plan de medidas de prevención y respuesta.

La jornada ha finalizado con una mesa redonda en la que los participantes han podido resolver dudas.

El objetivo principal de MEDUSA, proyecto que empezó en julio de 2014 y que está previsto que finalice en julio de 2016, es el diseño de metodologías de evaluación de riesgos para las Infraestructuras Críticas de Información, abordando los diversos efectos "en cascada" asociados con los incidentes en la seguridad que suceden a partir de la interacción entre entidades a lo largo de la cadena de suministro en múltiples niveles (infraestructura, nacional, intersectorial, etc.).