El port de València a l'avantguarda de la ciber-seguretat a través del projecte MEDUSA

València, 6 de maig de 2016.- Aquest matí s'ha celebrat, en les instal·lacions de l'Autoritat Portuària de València (APV), la conferència internacional **"Cyber-security in the Supply Chain: New approaches and challenges**", organitzada en el marc del projecte MEDUSA, cofinançat per la DG HOME - Comissió Europea - a través del Programa de Prevenció, preparació i gestió de les conseqüències del terrorisme i altres riscos relacionats amb la seguretat.

La jornada, organitzada per la APV, la Fundació Valenciaport i Feports, que participen en el projecte com a membres de l'Agrupació Europea d'Interès Econòmic - EUROPHAR, ha sigut inaugurada pel director de Seguretat i Medi ambient de la APV, Federico Torres i pel director general de la Fundació Valenciaport, Vicente del Rio. Federico Torres durant la seua intervenció ha destacat la participació de la APV en diferents projectes de seguretat així com l'engegada d'iniciatives pioneres com el CSI (Container Security Management), MEGAPORTS o la certificació de la ISO 28000. Per la seua banda, Vicente del Rio ha assenyalat que la Fundació Valenciaport, com a membre de EUROPHAR, és conscient de la importància que té la seguretat, tant física com a cibernètica, dins de la cadena logística portuària, per a garantir l'eficiència i la competitivitat de les economies nacionals. I és per açò, que s'involucra en projectes de cooperació d'àmbit europeu, com el projecte MEDUSA.

A continuació, Christos Douligeris, professor de la Universitat del Pireo, ha presentat els principals resultats del projecte MEDUSA:

• Una eina orientada a avaluar els riscos relacionats amb les infraestructures de la informació i comunicació que interaccionen al llarg de la cadena de subministrament

• Una proposta de mesures de prevenció i de resposta davant la detecció de qualsevol amenaça identificada en qualsevol node de la cadena logística

• Una descripció dels escenaris tipus més rellevants amb la finalitat d'avaluar l'eina, basats en el transport de contenidors, vehicles i GNL.

La jornada ha continuat amb les intervencions de Fernando Seco, director consultor de S2 Grup, que ha impartit una ponència sobre la ciber-seguretat en la cadena de subministrament i Rafael Pedrera, director d'operacions de l'Oficina de Ciber-Coordinació del Centre Nacional Per a les Infraestructures Crítiques (CNPIC) i Alfonso Ruiz, de la mateixa entitat, que han parlat sobre la protecció de les infraestructures portuàries crítiques.

A continuació, Manuel Esteve, director del Laboratori de Sistemes en Temps Real de la UPV, ha presentat un sistema de control i gestió de comandament integrat amb l'aplicació de noves tècniques de visualització per a mostrar l'ambient real i el ciberespai.

Per la seua banda, Pablo Noval, director tècnic de Saggas, ha descrit el flux de la cadena de transport del gas natural liquat detallant els diferents actors que participen en la cadena de subministrament.

Els riscos i desafiaments de la cadena logística del transport de contenidors han sigut presentats per José Gisbert, Responsable de Tecnologies de la Informació de MSC Terminal València. Gisbert ha explicat les relacions que manté una terminal de contenidors amb els agents externs de la cadena de subministrament, les normatives a seguir per a garantir la seguretat, els principals riscos i amenaces als quals s'exposen i què fer per a mitigar-los.

Durant la sessió de demostracions, Spyros Papastergiou, del Centre de Recerca de la Universitat de Pireo, ha presentat el "MEDUSA Toolkit", una eina que ha sigut dissenyada i desenvolupada en el marc del projecte i que permet una anàlisi exhaustiva de riscos i amenaces, tant físiques com a cibernètiques, tenint en compte el "efecte trencada" de tot el procés de transport a través de la identificació de tots els fluxos d'intercanvi d'informació entre els nombrosos sistemes de comunicació existents.

Per la seua banda, Stefan Schauer, del departament de Seguretat i Protecció digital de l'Institut Tecnològic d'Àustria, ha presentat MITIGATE, un projecte afavorit pel programa H2020, que el seu objectiu és crear un sistema que permeta avisar de qualsevol risc cibernètic, informant del nivell d'importància així com un pla de mesures de prevenció i resposta.

La jornada ha finalitzat amb una taula redona en la qual els participants han pogut resoldre dubtes.

L'objectiu principal de MEDUSA, projecte que va començar al juliol de 2014 i que està previst que finalitze al juliol de 2016, és el disseny de metodologies d'avaluació de riscos per a les Infraestructures Crítiques d'Informació, abordant els diversos efectes "en cascada" associats amb els incidents en la seguretat que succeeixen a partir de la interacció entre entitats al llarg de la cadena de subministrament en múltiples nivells (infraestructura, nacional, intersectorial, etc.).