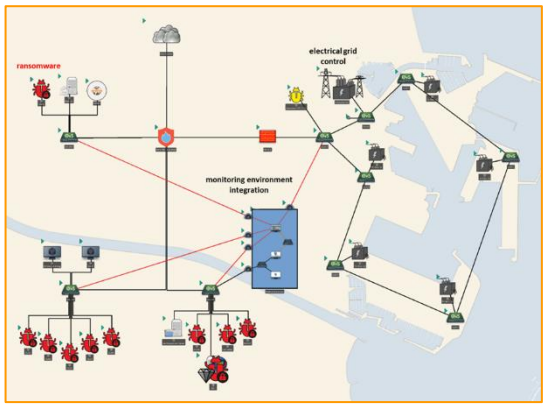
Piloto 1: Fuentes de energía en el puerto de Valencia

Descripción

El primer escenario piloto consistió en probar y validar una versión inicial del sistema Cyber-MAR en el ámbito de un escenario de ciberataque a la red eléctrica de la autoridad portuaria, en el Puerto de Valencia. El escenario se centró en la simulación de un ataque de acceso remoto a la infraestructura TI, TO, y red eléctrica del Puerto de Valencia. El objetivo principal de este ataque era cortar el suministro de energía al puerto, apagando el sistema TO de administración de la red, desde el ordenador del administrador TO, como punto de infección de origen. El objetivo secundario era simular un ataque de ransomware desencadenado por el servidor Command & Control, que bloquearía con criptografía todas los servidores y equipos de trabajo dentro de la infraestructura del puerto. Durante la demostración, el Cyber-Range de Cyber-MAR proporcionó información sobre el escenario desde diferentes puntos de vista: desde la perspectiva de un atacante y desde la perspectiva de un defensor utilizando el Sistema de Detección de Intrusiones (IDS) y SIEM.

Objetivos

- Adecuar los sistemas para evitar ciberataques a la red eléctrica portuaria.
- Mitigar las consecuencias en caso de un ataque.
- Restaurar el sistema en caso de un ataque.
- Sensibilizar al personal portuario sobre estas situaciones.
- Brindar capacitación y las habilidades necesarias en ciber amenazas.
- Brindar capacitación para una respuesta rápida en caso de emergencia.
- Posibilidad de adaptar los conocimientos proporcionados por este escenario en otras redes de media y baja tensión.



Topología piloto Valencia: Integración de IDS, XL-SIEM y MISP

Realización

El evento piloto de Valencia tuvo lugar el 16.12.2020, virtualmente a las 10.00-13.00 CET, vía zoom meeting.

Material

El material del piloto 1 del proyecto Cyber-MAR está disponible en la siguiente URL: https://www.cyber-mar.eu/event/cyber-mar-valencia-pilot-event-material-access/

Cyber-MAR de un vistazo

Título: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

Projecto ID: 833389

Coordinador: Instituto de Comunicaciones y Sistemas Informáticos (ICCS), Grecia

www. cyber-mar.eu
Cyber_MAR
Cyber-MAR
info@lists.cyber-mar.eu

Consorcio

Este proyecto ha recibido financiación del programa de investigación e innovación Horizonte 2020 de la Unión Europea en virtud del acuerdo de subvención n.º 833389. El contenido de este material refleja únicamente la opinión de los autores y la Comisión Europea no es responsable del uso que pueda hacerse de la información que contiene. contiene.