[CSIOT] Tema 1: Introducción a la Ciberseguridad Industrial

La ciberseguridad industrial es una disciplina de la ciberseguridad que incluye al conjunto de acciones que permiten defender entornos industriales. Generalmente la mayoría de la información existente se centra en ICSs y SCADAs de una red industrial.

Conceptos importantes

La infraestructura crítica es uno de los conceptos más importantes, es una infraestructura cuyo funcionamiento es demasiado esencial, suponiendo cualquier tipo de perturbación de estas infraestructuras un gran impacto en la sociedad (Centrales eléctricas, etc…)

Servicio esencial: su provisión mantiene el funcionamiento normal de una sociedad (Agua corriente, electricidad, sanidad…) un servicio esencial puede ser:

- Administración (Secuestro de sistemas del sepe, ayuntamientos….)
- Agua
- Alimentación Comunicaciones

Estos servicios esenciales funcionan sobre infraestructuras estratégicas, que pueden tener alternativas, pero si no funcionan pueden producir un gran problemas de bienestar, como es el caso de los hospitales, de forma que si fallan sus sistemas, miles de personas tendrían que ir a otros hospitales.

Políticas de seguridad industrial

Conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras industriales con el fin de prevenir, neutralizar y mitigar el daño causado por un ataque deliberado contra dichas infraestructuras. Esta políticas no solo definen pautas de ciberseguridad, si no que definen todo un ecosistema industrial.

Ley de Protección de Infraestructuras Críticas (PIC)

Es la normativa legal que rige dos cuestiones básicas: catalogar el conjutno de estructuras críticas que prestan servicios esenciales y las medidas a tomar para proteger frente a ataques. Principales aportaciones de la ley PIC:

- Se crea el sistema nacional de protección de infraestructuras críticas
- Catálogo nacional de infraestructuras críticas: Indica el número de instalaciones críticas en España que pertenecen a los sectores de energía, transporte, alimentos, aeroespacial, informática…
- El CERT se encarga de responder y coordinar en caso de un ciberataque.

Operadores críticos: Empresas que usan infraestructuras críticas pero no pertenecen al estado, como Telefónica, Repsol e Iberia.

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:csiot:tm1&rev=1738686718

Last update: **2025/02/04 16:31**