sop_ot_security

OT Zibersegurtasun Prozedura (Purdue Eredua)

1. Helburua

Fabrikako kontrol sistemen (ICS) segurtasuna bermatzea, ekoizpenaren jarraitutasuna eta langileen segurtasun fisikoa babesteko.

2. Arkitektura Segurua (Purdue Eredua)

- **Maila 4 (Enpresa Sarea):** ERP, Emaila, Web sarbidea.
- **Maila 3.5 (DMZ Industriala):** Historialariak, Patch zerbitzaria, Jump Host.
- **Maila 3 (Ekoizpen Operazioak):** SCADA zerbitzariak, HMIak.
- **Maila 2 (Kontrol Sarea):** PLCak, RTUak.
- **Maila 1/0 (Prozesua):** Sentsoreak, Aktuadoreak, Robotak.

3. Segurtasun Arauak

3.1 Sare Segmentazioa

- IT eta OT sareen arteko komunikazio zuzena **Debekatuta**.
- Komunikazio guztia DMZ industrialaren bidez egin behar da.
- Erabili suebakiak maila bakoitzaren artean (North-South trafikoa).

3.2 Urruneko Sarbidea

- Ez erabili TeamViewer edo antzeko tresnarik zuzenean PLCetara.
- Sarbidea **VPN seguru** bidez eta **MFA** (Multi-Factor Authentication) erabiliz soilik baimenduko da.
- Konexioa “Jump Host” baten bidez egin behar da DMZan.

3.3 Gailu Eramangarriak (USB)

- Debekatuta dago USB memoria pertsonalak OT ekipoetan konektatzea.
- Erabili “Kiosko” estazioak USBak eskaneatzeko malware bila konektatu aurretik.

3.4 Eguneraketak

- OT sistemak ez eguneratu automatikoki.
- Probatu partxeak laborategiko ingurunean lehenengo.
- Planifikatu mantentze-leihoak eguneraketetarako.