IEC 62443

IEC 62443 er en international standard, der omhandler cybersikkerhed i industrielle automatiserings- og kontrolsystemer (IACS). Standarden er udviklet af ISA (International Society of Automation) og vedtaget som IEC-standard. Den er struktureret i fire hovedområder, som hver især adresserer specifikke aspekter af cybersikkerhed. Herunder får du en struktureret oversigt i punktform, som giver en grundig forståelse af hele standarden.

🔍 1. Generelle begreber og modeller (IEC 62443-1-x)

Disse dele introducerer grundlæggende principper og terminologi for standarden.

- **62443-1-1: Terminologi og begreber**
  - Definerer centrale begreber som *IACS*, *zoner*, *konduitter*, *trusselsaktører* og *risikovurdering*.
  - Forklarer forskellen mellem IT-sikkerhed og OT-sikkerhed.
- **62443-1-2: Metrikker til vurdering af overholdelse**
  - Beskriver, hvordan man måler overholdelse af sikkerhedskrav i IACS.
- **62443-1-3: Systemlivscyklus og sikkerhedsmodeller**
  - Introducerer livscyklusmodellen for systemer: design, implementering, drift og vedligeholdelse.
  - Beskriver "Defense-in-Depth"-tilgangen og *Zonemodellen* for segmentering.

🛡 2. Politikker og procedurer (IEC 62443-2-x)

Fokus på ledelse, politikker og organisatoriske procedurer for at opnå og vedligeholde cybersikkerhed.

- **62443-2-1: Krav til sikkerhedsstyringssystemet (CSMS)**
    - Beskriver, hvordan organisationer opbygger og vedligeholder et *Cyber Security Management System*(CSMS).
    - Inkluderer politikker, risikovurdering og beredskabsplaner.
- **62443-2-2: Systemvurdering og rapportering**
    - Krav til vurdering og rapportering af systemers sikkerhedsstatus.
- **62443-2-3: Patch Management**
    - Beskriver processen for sikker administration af opdateringer og patches i industrielle systemer.
- **62443-2-4: Krav til serviceleverandører**
    - Definerer sikkerhedskrav til tredjepartsleverandører og integratorer.

⚙ 3. Systemkrav (IEC 62443-3-x)

Teknisk fokus på systemdesign og -implementering, herunder risikobaseret beskyttelse.

- **62443-3-1: Sikkerhedsteknologier for IACS**
    - Introducerer sikkerhedsteknologier som firewalls, VPN'er, adgangskontrol og segmentering.
- **62443-3-2: Risikovurdering og systemdesign**
    - Metodologi for *Zonemodellering* og *konduitsegmentering*.
    - Krav til beskyttelse af kritiske systemer baseret på risikoniveau.
- **62443-3-3: System sikkerhedskrav og sikkerhedsniveauer (SL)**
    - Introducerer *Sikkerhedsniveauer (SL)* fra SL 0 til SL 4:
        - SL 0: Ingen sikkerhed
        - SL 1: Beskyttelse mod utilsigtede hændelser
        - SL 2: Beskyttelse mod simpel bevidst hacking
        - SL 3: Beskyttelse mod avanceret målrettet angreb
        - SL 4: Beskyttelse mod statsaktør-lignende trusler

🔲 4. Komponentkrav (IEC 62443-4-x)

Omhandler tekniske krav til individuelle komponenter og produktudvikling.

- **62443-4-1: Sikker udviklingslivscyklus (SDL)**
    - Krav til udvikling af sikre produkter, herunder:
        - Sikker kodning
        - Sårbarhedstestning
        - Dokumentation af sikkerhedsfunktioner
    - Fokus på *Secure by Design* og *Secure by Default* principper.
- **62443-4-2: Tekniske sikkerhedskrav til komponenter**
    - Specificerer sikkerhedskrav for enheder som PLC'er, RTU'er, SCADA-systemer og HMI'er.
    - Omfatter:
        - Identitetsstyring og autentificering
        - Kryptering af data i transit og i hvile
        - Logning og hændelseshåndtering

📈 5. Praktisk anvendelse og implementering

For at blive ekspert er det vigtigt at forstå, hvordan man implementerer IEC 62443 i praksis:

- **Risikobaseret tilgang:** Udfør risikovurderinger baseret på systemets kritikalitet og trusselsbilledet.
- **Zonemodellering:** Opdel netværket i sikre zoner baseret på systemfunktion og sikkerhedsniveau.
- **Defense-in-Depth:** Implementér flere lag af beskyttelse, herunder netværkssegmentering, adgangskontrol og overvågning.
- **Sårbarhedsstyring:** Overvåg, vurder og håndter sårbarheder løbende.
- **Incidenthåndtering:** Opret beredskabsplaner og øv håndtering af hændelser.

🎭 6. Vigtige principper og begreber

Nogle af de mest centrale principper i IEC 62443 omfatter:

- *Least Privilege*: Brugeren eller systemet får kun de rettigheder, der er nødvendige for opgaven.
- *Defense-in-Depth*: Lagdelt sikkerhed for at minimere konsekvenserne af en brist.
- *Zonering og Konduit*: Segmentering af netværket for at begrænse angrebsoverfladen.
- *Secure by Design*: Sikkerhed tænkes ind fra starten i designfasen.

Thank You!

We respect your valuable time with NTO

If you have any questions, please reach us