TUOTANNON KYBERTURVALLISUUS-KYVYKKYYDEN YLEISKARTOITUKSEN SUUNNITTELUN TARKASTUSLISTA

Tuotannon kyberturvallisuuskyvykkyyden yleiskartoituksen suunnittelun tarkastuslista

Tämä kysymyslista on tarkoitettu energiayritysten käyttöön niiden suunnitellessa tuotannon kyberturvallisuuskyvykkyyden yleiskartoitusta.

Oletteko muodostaneet organisaatiossanne kyberturvallisuuden, tietoturvallisuuden, tai kokonaisturvallisuuden tiimin, jonka vastuulle kuuluu tietoturvan kehittäminen ja valvonta?

- Onko organisaation johto sitoutunut kyberturvallisuuden kehittämiseen?
  - Miten sitoutuminen näkyy henkilöstön työajan resursoinnissa?
  - Onko kyberturvallisuus säännöllisesti johdon käsiteltävänä?
    - Onko automaatioympäristöjen kyberturvallisuus säännöllisesti johdon käsiteltävänä?

- Onko kehitystiimissä mukana henkilöitä kaikilta automaation kannalta kriittisiltä osa-alueilta, esimerkiksi
  - tuotannon (automaation) kunnossapidosta ja kehittämisestä,
  - yritys- ja laitostason ICT-järjestelmien ylläpidosta ja kehittämisestä,
  - automaation hankinnoista,
  - tuotannon järjestelmien pääkäyttäjistä,
  - kokonaisturvallisuudesta ja sen kehittämisestä, ja
  - henkilö- ja ympäristöturvallisuuden kehittämisestä?

Oletteko määritelleet tuotannon kyberturvallisuuskyvykkyyden yleiskartoituksen tavoitteet?

- Onko tavoitteena tunnistaa kyberturvallisuuden kehittämiskohteet yleisesti?
  - Vai keskitytäänkö vain tiettyihin tuotantojärjestelmiin?

Oletteko valinneet kartoituskohteen?

- Mitä dokumentaatiota kohteesta toimitatte kartoittajille?
  - Toimitatteko tietoturvapolitiikoita ja käytäntöjä kuvaavaa materiaalia?
  - Toimitatteko teknistä materiaalia kuten verkkokuvia ja inventaarioraportteja?

Oletteko määritelleet mitä menetelmiä kartoittaja saa käyttää ja mitä menetelmiä hänen pitää käyttää kartoituksen aikana?

- Tehdäänkö kartoituksen aikana passiivisia toimenpiteitä kuten esimerkiksi
  - dokumentoinnin katselmuksia,
  - haastatteluja ja
  - avointen lähteiden tiedustelua (*Open-Source Intelligence* OSINT).

- Tehdäänkö kartoituksen aikana aktiivisia toimenpiteitä kuten
  - haavoittuvuusskannausta,
  - penetraatiotestausta (tunkeutumistestaus),
  - kohteessa olevien langattomien verkkojen analysointia,
  - sosiaalista manipulointia,
  - verkkoliikenteen tallennusta ja analyysiä,
  - ohjelmistojen lähdekoodin analyysiä,
  - lokien tutkimista,
  - palomuurisääntöjen tutkimista, tai
  - häiriönhallintaprosessien testaamista testisyötteillä.

Oletteko valinneet sekä hallinnolliset että tekniset henkilöt, jotka kartoittaja haastattelee kartoituksen aikana?

Hallinnollisiin vaatimuksiin kuluu:

- automaation tietoturvatietoisuus,
- automaation tietoturvaan liittyvä raportointi ja rekisterit,
- automaatio-omaisuuden hallinta,
- automaation käyttäjien hallinta ja käyttöoikeudet,
- automaation häiriötilanteesta toipuminen ja
- automaation tietojärjestelmien ja sovelluksien hallinta, kehitys ja ylläpito.

Teknisiin vaatimuksiin kuuluu:

- automaation omaisuuden hallinta,
- automaation päivitysten ja muutostenhallinta,
- automaatioverkon turvavyöhykkeet ja datan suodatus.
- automaatioverkon pääsynvalvonta,
- automaationverkon suojaaminen haittaohjelmia vastaan,
- automaatiojärjestelmän varmuuskopiointi ja niistä palauttaminen ja
- automaation fyysinen suojaus.

Oletteko suunnitelleet missä tiloissa kartoittajat käyvät tutustumassa valittuihin kohteisiin?

Oletteko valinneet henkilöt jotka esittelevät valitun kartoituskohteen verkkoarkkitehtuurin ja vastaavat tarvittaessa kartoittajien kysymyksiin?