Tietoturvakysely sähköverkkoon liittyville voimalaitoksille ja sähkövarastoille

1 Tavoitteet

Tässä dokumentissa esitetyillä kysymyksillä pyritään varmistamaan tietoturvan perustaso sähköverkkoon liittyvällä B, C tai D tyypin voimalaitoksella tai sähkövarastolla. Tietoturvallinen toiminta vahvistaa kantaverkon käyttövarmuutta.

Kysymykset koskevat voimalaitoksen tai sähkövaraston järjestelmiä kokonaisuudessaan sisältäen myös laitosta operoivien ja ylläpitävien tahojen järjestelmät ja tietoliikenneyhteydet (esim. tuulivoimalaitoksen turbiinitoimittaja tai voimalaitoksen käytöstä etäohjauksella vastaava toimija).

Vastauksien tulee sisältää lyhyt kuvaus jokaisesta kysytystä aiheesta kuitenkaan vaarantamatta tietoturvaa liian tarkalla vastauksella. Vastaus toimitetaan Fingridille vapaamuotoisesti laadittuna tekstiasiakirjana osana järjestelmäteknisten vaatimusten edellyttämää tiedonvaihtoa (VJV2024: luku 10.3.6, SJV2024: luku 10.3.7).

Kysely täytetään kahdesti. Suunnitteluvaiheessa (ennen väliaikaisen käyttöönottoilmoituksen myöntämistä) kuvataan, miten asiat aiotaan huomioida suunnittelussa. Käyttöönottovaiheen jälkeen (ennen lopullisen käyttöönottoilmoituksen myöntämistä) kuvataan toteutettu ratkaisu.

Kysymykset on laadittu pääasiallisesti SANS instituutin The Five ICS Cybersecurity Critical Controls /1/ dokumentin pohjalta.

2 Kysymykset

2.1 Tietoturvapoikkeamiin reagointi

- Onko liittyjällä tietoturvapoikkeamanhallinnan suunnitelma, joka huomioi tuotannon tietojärjestelmien (Operational Technology, OT) ominaispiirteet?
- Onko suunnitelma harjoiteltu?

2.2 Verkon segmentointi ja puolustettava arkkitehtuuri

- Onko liittyjän laitoksen tietoliikenneverkko segmentoitu loogisesti/fyysisesti?
- Onko tietoliikenneverkon segmenttien välinen liikennöinti rajoitettu vain järjestelmän toiminnan kannalta välttämättömään liikenteeseen?
- Onko laitteista suljettu järjestelmän toiminnan kannalta turhat tietoliikenneportit ja palvelut?

2.3 Verkkoliikenteen monitorointi

- Monitoroidaanko laitoksen tietoliikenneverkkoa sinne kuulumattoman tai poikkeavan liikenteen havaitsemiseksi?
- Onko liittyjällä listaus laitteista, jotka on kytketty laitoksen tietoliikenneverkkoon?

2.4 Suojatut etäyhteydet

- Onko laitoksen tietoliikenneverkkoon mahdollista ottaa etäyhteys ulkopuolisesta verkosta?
- Vaaditaanko etäyhteyden muodostamisen jossain vaiheessa käyttäjältä monivaiheista tunnistautumista?
    - Esimerkiksi, vaaditaanko jossain kohtaa kirjautumisprosessia monivaiheista tunnistautumista, kun käyttäjä tunnistautuu käytöstä vastaavan tahon käytönhallintajärjestelmään?
    - Esimerkiksi, vaaditaanko jossain kohtaa kirjautumisprosessia monivaiheista tunnistautumista, kun käyttäjä tunnistautuu paikalliseen ohjausjärjestelmään?

2.5 Haavoittuvuuksien hallinta

- Onko liittyjällä lista tietoliikenneverkkoon liitettyjen laitteiden ohjelmisto- ja laiteohjelmistoversioista?
- Miten liittyjä seuraa näihin kohdistuvia haavoittuvuuksia?
- Onko liittyjällä suunnitelma haavoittuvuuksien aiheuttamien riskien rajaamiseen?
- Onko liittyjä sopinut laitteiden ylläpitovastuista?

2.6 Käyttäjien hallinta

- Onko laitoksen tietoliikenneverkkoon kytketyissä laitteissa vaihdettu oletuskäyttäjätunnusten salasanat?
- Onko käyttäjä- ja ylläpitotason tunnukset eroteltu aina kun mahdollista?
- Onko laitoksen laitteissa käytettyjen tunnusten elinkaari hallittu?

2.7 Etäohjattavan laitoksen yhteyksien varmennukset

- Kuinka etäohjattavan laitoksen ohjausyhteydet on varmistettu yksittäisen vian varalta?
- Kuinka pitkä toiminta-aika alueellisen jakeluverkon sähkökatkossa etäyhteyksissä on?

2.8 Palautuminen

- Onko liittyjällä suunnitelma palautumiseen laite- tai konfiguraatio viasta?
- Onko liittyjällä ajan tasaiset varmuuskopiot laitteiden konfiguraatioista?

Viitteet

/1/ The Five ICS Cybersecurity Critical Controls https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/ viitattu 2.11.2023