AUDITOINTIKUMPPANIN VALINNAN TARKASTUSLISTA

Kuva: Tumisu/Pixabay

AUDITOINTIKUMPPANIN VALINNAN TARKASTUSLISTA

Tämä kysymyslista on tarkoitettu energiayritysten käyttöön niiden suunnitellessa kyberturvallisuusauditointia.

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

- Kuuluuko tiimin vastuulle kyberturva-auditointien suunnittelu ja organisointi?
- Onko turvallisuustiimissä mukana henkilöitä kaikilta automaation kannalta kriittisiltä osa-alueilta?
    - tuotannon (automaation) kunnossapidosta ja kehittämisestä,
    - yritys-, laitos- ja sähköverkkojen ICT-järjestelmien ylläpidosta ja kehittämisestä,
    - automaation hankinnoista,
    - tuotannon järjestelmien pääkäyttäjistä,
    - kokonaisturvallisuudesta ja sen kehittämisestä, ja
    - henkilö- ja ympäristöturvallisuuden kehittämisestä?

Tunteeko auditointikumppanin tiimi kyberturvallisuuden merkityksen toimialanne kokonaisturvallisuudelle ja tuotannon luotettavuudelle?

Turvalliseen toimintaan kuuluvat esimerkiksi

- koko henkilöstön kyberturvallisuustietoisuuden kehittäminen,
- jatkuvuutta ja turvallisuutta tukevien toimintaohjeiden ja lupamenettelyjen käyttöönottaminen,
- tuotannon suojauskonseptien jatkuva kehittäminen ja käyttäminen,
- kyky tunnistaa teihin kohdistuvaa vakoilua ja tietomurtoja,
- jatkuva toteutuneiden häiriöiden, tehtyjen virheiden ja epäiltyjen hyökkäysten raportointi ja seuranta,
- häiriöistä palautumisen suunnittelu ja toistuva harjoitteleminen, sekä
- uusien varautumistapojen etsiminen ja käyttöönottaminen kyberuhkien muuttuessa yhä vaikeammin havaittaviksi.

AUDITOINTIKUMPPANIN ARVIOINTI JA VALINTA

Tarkastuslista

Tunteeko auditointikumppanin tiimi teidän toimialanne kyberuhat?

- Millaisia uhkia ja tietoturvaloukkauksia on esiintynyt teidän toimialallanne ja käyttämänne kaltaisissa järjestelmissä?
- Oletteko saamaa mieltä liiketoimintanne riskeistä ja uhkista auditointikumppanin kanssa?

Pystyttekö kertomaan auditointikumppanille automaatiojärjestelmiinne kuuluvien ohjausten ja laitteiden sijainnin sekä niiden ominaisuudet?

- Miten tiedot on dokumentoitu ja miten ne pidetään ajan tasalla?
    - Miten tietoja päivitetään? Mitä työkaluja käytetään?
    - Ovatko tiedot käytettävissä tietoteknisen tai tietoliikennehäiriön sattuessa?
- Mitkä laitteet käyttävät analogia- ja mitkä digitaalitekniikkaa?
- Mitkä laitteet ovat kytkettävissä tai kytketty IP (*Internet Protocol*) -verkkoon?
    - Mitkä laitteet ovat saavutettavissa IP-yhdyskäytävien kautta?
- Miten ja mitä verkkoja käyttäen laitteet on kytketty toisiinsa?
    - Onko järjestelmästä piirretty ajantasainen verkkokaavio?
        - Miten verkkokaaviota pidetään yllä ja kenen vastuulla ylläpito on?
- Mitkä laitteista sijaitsevat suojatuissa ja/tai valvotuissa tiloissa? Ja mitkä eivät?
- Mitkä ohjauslaitteet ovat viranomaismääräysten alaisia?
- Miten auditointikumppani kykenee pitämään nämä tiedot luottamuksellisina kaikissa olosuhteissa? Millainen NDA sopii auditointikumppanille?

Mitkä ovat toimintanne kriittiset osat kannattaa antaa ulkoisen osapuolen auditoitaviksi?

- Onko automaatiojärjestelmällenne jo tehty kyberturvallisuusnäkökulman sisältävä riskinarviointi?
- Minkä järjestelmän osien tai laitteiden häiriö tai menettäminen voi aiheuttaa merkittäviä vaaroja ihmisille, ympäristölle tai organisaation taloudelliselle jatkuvuudelle?

Oletteko määritelleet yhdessä omistajien kanssa mihin järjestelmiin auditointi rajataan?

- Mitä kriteerejä valinnassa käytetään?
- Miten rajaukset on dokumentoitu?

Oletteko määritelleet yhdessä omistajien kanssa tavoitteet valittujen kohteiden auditoinnille?

- Miten ja mihin tavoitteet on dokumentoitu?

Oletteko määritelleet alustavat vaatimukset auditointitoimittajien kyvykkyyksille?

- Oletteko kysyneet mahdollisilta toimittajilta heidän kyvykkyyksiään ja referenssejään?
- Käytättekö ulkopuolista apua valitessanne auditointitoimittajia?

Koestatteko useampia mahdollisia toimittajia auditointipiloteissa?

- Oletteko valinneet auditointipilottien kohteet?
- Miten arvioitte auditointitoimittajien toimintaa pilotissa?
    - Käytättekö ulkopuolista apua toimittajien arvioinnissa?

Onko teillä järjestelmiä tai niiden osia, joiden auditointi vaatii erityisosaamista?

- Miten varmistatte sen, että valitsemallanne auditointitoimittajalla on vaadittava erityisosaaminen?

Kenelle jaatte tietoa auditoinnin tuloksista?

- Onko teillä prosessi, jota käytätte auditointien kehittämiseen?
    - Miten hyödynnätte aiemmista auditoinneista saatuja kokemuksia?

Auditoinnin tulokset ovat luottamuksellisia.

Yksityiskohtaiset tiedot paljastaisivat miten juuri teitä vastaan hyökättäisiin tehokkaasti.