OMAISUUDEN HALLINNAN

Tarkastuslistat

OMAISUUDEN HALLINNAN TARKASTUSLISTAT

Kenelle nämä listat on tarkoitettu?

- ***järjestelmävastaaville***
- ***hankinnoista vastaaville henkilöille***
- ***hankintaosastolle***
- ***hankintoihin osallistuville asiantuntijoille***
- ***sisäiselle valvonnalle***

Mihin tämä lista on tarkoitettu?

- ***Listan tarkoitus on tuoda esiin hankintojen tärkeys riittävän kyberturvallisuuden tason mahdollistajana koko hankittavan kohteen elinkaaren ajan.***

Hankinnoilla on erittäin suuri rooli omaisuuden hallinnan onnistumisessa. Hankintasopimuksen yhteydessä on määriteltävä vaatimukset myös kyberturvallisuudelle, sillä jälkeenpäin kohteen turvallisuutta voi olla tuotannollisista syistä lähes mahdotonta tai erittäin kallista korjata.

Tässä listassa termejä kyberturvallisuus ja tieto-turvallisuus käytetään synonyymeinä.

Onko hankintasopimuksessa määritelty toimitettavan järjestelmän kyberturvallisuusvaatimukset?

- Miten toimittaja pystyy täyttämään määritellyt vaatimukset?
- Kuka hyväksyy riskin, joka aiheutuu kyvyttömyydestä täyttää asetetut vaatimukset?
- Miten ja minne hyväksytty riski kirjataan?
- Kuka sovittaa vaatimukset osaksi yrityksen kyberturvallisuusmenettelyjä?

Onko kaikki toimituskokoonpanoon kuuluvat tuotteet ja palvelut yksilöity?

- Onko kaikkien näiden tietoturvaominaisuudet kuvattu tarkasti?
- Käytetäänkö toimituksen osana tietoturvatuotteita ja palveluita?
    - Mitä tuotteita kolmas osapuoli toimittaa?

Kuka vastaa toimitukseen kuuluvien tuotteiden huollosta ja ylläpidosta?

- Kuinka kauan ja millä ehdoilla?
- Miten elinkaaren hallinta on toteutettu?
    - Ehdottaako toimittaja elinkaarihallintaa vai onko toimituksen koko elinkaari suunniteltu myös tietoturvavaatimusten osalta?

Mitkä ovat toimituksen kriittisimmät osat joita pitää erityisesti huoltaa ja ylläpitää?

- Kuka arvioi kriittisten osien yhteisvaikutuksen osana yrityksen tietoteknistä infrastruktuuria?
- Kuka arvioi toimituksen yhteisvaikutuksen osana automaatiojärjestelmän tietoteknistä infrastruktuuria?

Miten toimitetun järjestelmän kyberturvallisuustilan seuranta on järjestetty?

- Tehdäänkö järjestelmälle auditointeja?
- Kuinka kauan seurantaa tehdään ja kenen toimesta?
- Miten toimittaja ilmoittaa tilaajalle, jos toimitetusta järjestelmästä tai jostain siihen kuuluvasta osasta löytyy haavoittuvuus?
- Miten tilaaja ilmoittaa toimittajalle, jos toimitetusta järjestelmästä löytyy haavoittuvuus?

Automaatio-omaisuuden hallinta kyberturvallisuuden näkökulmasta perustuu siihen, että tunnetaan tärkeimmät automaatioon kuuluvat osat sekä ymmärretään niiden ominaisuudet.

Tiedetäänkö kaikkien automaatioon kuuluvien ohjausten ja laitteiden sijainti ja ominaisuudet?

- Miten tiedot on dokumentoitu ja kuinka usein tietoja päivitetään?
  - Miten tietoja päivitetään? Mitä työkaluja siihen käytetään?
  - Miten tietoon pääsee käsiksi normaalitilanteessa?
  - Miten tietoon pääsee käsiksi erilaisissa häiriötilanteissa?
- Mitkä laitteet käyttävät analogia- ja mitkä digitaalitekniikkaa?
- Mitkä laitteet ovat kytkettävissä tai kytketty IP (*Internet Protocol*) verkkoon?
- Miten ja mitä verkkoja käyttäen laitteet on kytketty toisiinsa?
  - Onko järjestelmästä piirretty ajantasainen verkkokaavio
  - Onko järjestelmästä piirretty ajantasainen tietovuokaavio?
  - Miten kaaviot ylläpidetään ja kenen toimesta?
- Mitkä laitteista sijaitsevat suojatuissa ja/tai valvotuissa tiloissa? Ja mitkä eivät?
- Mitkä ohjauslaitteista ovat viranomaismääräysten alaisia?
- Mitkä mittauslaitteet tai -järjestelmät tuottavat viranomaisraportoinnin edellyttämää tietoa?

Mitkä ovat toiminnalle tärkeimmät ja kriittisimmät osat?

- Onko automaatiojärjestelmälle tehty riskiarviointi?
  - Sisältyykö tietoturva toiminnallisten riskien arviointiin?
- Minkä järjestelmän osien tai laitteiden häiriö tai menettäminen voi aiheuttaa merkittäviä vaaroja ihmisille, ympäristölle tai organisaation taloudelliselle jatkuvuudelle?

Miten automaatiojärjestelmän eri osien hallinnointi on järjestetty?

- Hallinnoiko automaation eri osia organisaation automaatio-osasto, IT-osasto, vai onko hallinta ulkoistettu?

Onko automaatiojärjestelmä kytketty yrityksen toimisto- tai konserniverkkoon tai muuhun ulkoiseen verkkoon tai onko automaatioon etäyhteys?

- Onko näiden yhteyksien riski automaatiojärjestelmälle arvioitu?

Miten haavoittuvuuksien hallinta on järjestetty?

Omaisuuden hallintaratkaisujen arvioinnin lyhyt tarkastuslista:

Soveltuvuus

- Miten omaisuuden hallintaratkaisun soveltuvuus omiin tarpeisiin on arvioitu?
  - Sopiiko ratkaisu esimerkiksi monitoimittajaympäristöön, omaan- tai ulkoistettuun käyttöön?
  - Onko käyttäjähallinta omissa käsissä vai palvelun tuottajalla?
    - Kuinka paljon manuaalista työtä käyttäjähallinta vaatii, jos se on palvelun tuottajalla?
  - Mitkä ovat rajapinnat yrityksen omiin järjestelmiin niin varsinaisen tiedon kuin käyttäjähallinnan näkökulmista?
- Onko käyttäjät otettu mukaan ratkaisun arviointiin ja valintaan?
  - Onko ratkaisun käytettävyyttä arvioitu?
  - Miten ratkaisu tukee eri tehtäviä organisaatiossa?
- Onko hallintaratkaisuun liittyvät riskit arvioitu?

Muutoksen hallinta

- Miten tieto kerätään hallintaratkaisuun?
  - Mitä prosesseja käytetään tiedon keräämiseen ja niiden ajantasaisena pitämiseen?
  - Kuka vastaa prosesseista?
  - Miten tietojen päivittäminen ja oikeuksien hallinta monitoimittajaympäristössä on vastuutettu?
    - Toimittajille? Omalle organisaatiolle?
    - Tuetaanko tietojen automaattista syöttöä?

Käytettävyys, käyttöönotto ja ylläpito

- Onko ratkaisun toimittaja luotettava?
  - Kotimainen toimittaja?
- Miten hallintaratkaisun ylläpito on järjestetty?
  - Kuinka pitkäksi aikaa?
- Miten hallintaratkaisusta saadaan tiedot ulos koneluettavassa ja dokumentoidussa muodossa?
- Onko hallintaratkaisussa automatisointia helpottavia rajapintoja?

Laajennettavuus tulevaisuuden tarpeisiin ja käyttö muualla

- Käyttääkö hallintaratkaisu standardirajapintoja?
- Löytyykö ratkaisulle sovellukset (apps) yrityksen kannalta tärkeimmille alustoille?
  - Mikä on sovellusten tuottama lisäarvo ts. miten niitä voidaan hyödyntää päivittäisessä toiminnassa?