START-UP TYÖPAJAN SUUNNITTELUN TARKASTUSLISTA

START-UP TYÖPAJAN SUUNNITTELUN TARKASTUSLISTA

Kenelle tämä lista on tarkoitettu?

- ***Tietoturvapäälliköille (kartoituksen koordinointi)***
- ***Liiketoimintajohdolle***
- ***Laitoksen ja yrityksen IT-vastuullisille***
- ***Turvallisuus- ja riskienhallintapäälliköille***
- ***Kehityspäällikölle***
- ***Kunnossapitovastaaville***
- ***Hankintavastaaville***

Mihin tämä lista on tarkoitettu?

- ***Start-up työpajan suunnittelun avuksi, jotta voidaan herättää henkilöstö kyberturvallisuuden tärkeyteen ja aloittaa yhteinen työskentely kyberturvallisuuden kehityskohteiden parissa.***
- ***Start-up työpajalla on erittäin suuri rooli kyberturvallisuustyön saamiseksi käyntiin yrityksessä.***

JOS ORGANISAATION JOHTO EI OLE YMMÄRTÄNYT KYBERTURVALLISUUSTYÖN TÄRKEYTTÄ, NIIN KYBERRISKIT PAHENEVAT JA TUOTANTO ALTISTUU KYBERHÄIRIÖILLE.

Onko organisaation johto sitoutunut kyberturvallisuuden kehittämiseen?

- Miten sitoutuminen näkyy käytännön resursoinnissa?
- Onko kyberturvallisuus säännöllisesti johdon käsiteltävänä?
    - Onko automaatioympäristöjen kyberturvallisuus säännöllisesti johdon käsiteltävänä?

Onko organisaatio määrittänyt tuotantonsa kyberturvallisuuden tärkeimmät kehityskohteet?

- Tarvitaanko erillinen tarvekartoitus ennen start-up työpajaa?
    - Ketkä organisaatiosta osallistuvat tarvekartoituksen tekemiseen? Tyypillisesti mukana ovat esimerkiksi
        - tietoturvapäällikkö (kartoituksen koordinointi),
        - liiketoimintajohto,
        - turvallisuus- ja riskienhallintapäällikkö,
        - kehitysvastaavat,
        - kunnossapitovastaavat, sekä
        - hankintavastaavat.
    - Tarvitaanko tarvekartoituksen tekemiseen ulkopuolista apua?
        - Millaista apua tarvitaan? Fasilitointi, projektipäällikkö, haastattelijat?

Mikä on start-up työpajan tavoite ja agenda?

Onko start-up työpajan aihe valittu? Suositeltavaa <u>on</u> keskittyä perusasioihin, jotta kypsyystasoa voidaan nostaa suunnitelmallisesti. Aiheina voivat olla esimerkiksi yksi tai useampi seuraavista

- Automaation kyberturvallisuuden kehitysryhmän perustaminen, tehtävät, vastuuttaminen ja työnjako.
- Mitä pitäisi tehdä etukäteen, jotta kyberhyökkääjät eivät onnistuisi? Osaaminen: miten yrityksessä saadaan aikaan tuotantoautomaation tietoturvahallinta ja tietoturvan jatkuva parantaminen?
- Miten selvittää tuotantoverkon kyberturvallisuustilanne? Mm. tuotantolaitokset, sähköverkko, kaukokäyttöverkko, etäyhteydet.
- Käyttö- ja päivystystoimen turvalliset etäyhteydet: Oma henkilöstö & kumppaneiden verkosto.
- Hankintasopimusten kyberturvallisuusvaatimukset, erityisesti automaation ja automaation tukijärjestelmien (esimerkiksi ulkoistettu IT) osalta.
- Ylläpitosopimusten kyberturvallisuusvaatimukset & automaatiojärjestelmien päivitykset ja vikakorjaukset.
- Yhteiskäyttötunnusten käyttö sekä käyttäjätunnusten ja salasanojen riittävä laatu.
- Tuotantoverkon segmentointi ja sen tärkeys.
- Automaation varmuuskopioinnin merkitys ja palautumistestaus.
- Automaation kyberturvallisuuden suunnitelmallinen tason nosto.

START-UP TYÖPAJAN SUUNNITTELU

Tarkastuslista

Ketkä osallistuvat työpajaan? Aihe vaikuttaa osallistujien valintaan ja päinvastoin.

- Hankitaanko työpajaan ulkopuolisia puhujia?
  - Oman toimialan edelläkävijöitä kertomaan omista kokemuksistaan ja toimimaan vertaistukena?
  - Kyberturvallisuusasiantuntijoita (ei myyntimiehiä) joilla on tietämystä toimialasta?

Onko aika ja paikka valittu sekä tiedotettu kaikille osallistujille hyvissä ajoin?

- Onko materiaalia mitä kannattaa jakaa etukäteen osallistujille tutustuttavaksi?

Onko palautteen kerääminen valmisteltu?

- Käytetäänkö esimerkiksi suullista palautetta vai kyselylomaketta?
- Miten ja keiden toimesta palaute käsitellään?

Mitä jatkotoimia on suunniteltu tehtäväksi työpajan jälkeen?

- Onko jatkotoimien vastuulliset määritelty?
- Miten jatkotoimien kehittymistä seurataan ja kenen toimesta?
- Onko johto sitoutunut jatkotoimien mahdollistamiseen esimerkiksi riittävän resursoinnin avulla?