Digi- ja kyberturvallisuuden huomioiminen yrityksen eri strategioissa 2021 / Kysymykset

Arvoisa vastaaja, yrityksen johto ja strategia-asiantuntija,

Tähän mennessä yritykset ovat investoineet merkittävästi digitalisaatioon Suomessa sekä kiinnittäneet toiminnassaan huomiota luottamukseen ja vastuullisuuteen. Kuitenkaan emme tarkkaan tiedä, miten digitalisaatioon tehdyt investoinnit ovat vaikuttaneet yrityksen strategiatyöhön tai liiketoimintastrategiaan, luotettavuuteen ja vastuullisuuteen, eikä miten kyberturvallisuus tukee yrityksen liiketoimintastrategian toteutumista käytännössä?

Digipoolin 2020 toteuttaman selvityksen mukaan kotimaisten yritysten liiketoimintastrategiset linjaukset voisivat tukea toimeenpanoa vielä paremmin.

Projektin kokonaistavoitteena on tuottaa toteuttamiskelpoisia kehittämis- ja toimeenpanoehdotuksia tukemaan yrityksien hallituksia, johtoa ja johtoryhmiä ottamaan huomioon kyberturvallisuus yritysten strategiaprosesseissa ja johtamisessa.

Tämä kysely on tarkoitettu kaikille yrityksille koosta riippumatta. Kysely on kertaluonteinen ja sillä saadut tulokset käytetään Digipoolin projektin lähtötietoina. Kyselyn toteuttamisesta vastaa Cyberwatch Oy.

Kyselytutkimuksen tavoitteena on selvittää, mitä yritysjohtajat ajattelevat, tuntevat, kokevat tai uskovat oman yrityksen kyberturvallisuuden tasosta ja kehittämistoimista osana strategiaprosesseja sekä liiketoimintaa. Tämä tutkimus toteutetaan kyselylomakkeella netissä kaikille yrityksille, sekä erikseen kutsuttavilla haastatteluilla.

Kysymyssarjalla kartoitetaan yrityksen johtamista strategiselta tasolta tämän päivän tapahtumiin saakka. Tavoitteena on löytää ne ***strategiatyön tai vastaavan menettelyn*** lähtökohdat ja prosessien osatekijät, jotka mahdollistavat strategisen tason kulttuurin, tavoitemäärittelyn ja toimintakyvyn.

Tulokset käsitellään anonyymisti. Käsittelemme saamiamme tietoja salassa pidettävänä tietona.

Tulosten käsittelyyn ja tilastointiin liittyviä taustakysymyksiä on 9 kpl ja varsinaisia kysymyksiä 52 kpl. Raportoinnin onnistumisen varmistamiseksi täytättehän ensimmäiselle sivulle tarvittavat taustatiedot huolellisesti. Kysymykset on jaoteltu seuraaviin viiteen osioon:

1. Taustatiedot (9 kpl, joista osa vapaaehtoisia)
2. Yrityksen strategiantyön lähtökohdat (14 kpl)
3. Yrityksen strategiatyö (9 kpl)
4. Yrityksen strategian toimeenpano ja tulosten mittaaminen (12 kpl)
5. Yrityksen digi- ja kyberturvallisuustoimenpiteiden nykytilanne (17 kpl)

Vastaukset osioihin 2–5 annetaan seuraavan neliportaisen asteikon mukaan:

- **täysin toteutettu**, yritys voi todeta ja osoittaa, että kysyttävä asia on sen oman arvioinnin mukaan toteutettu riittävän hyvin
- **osittain toteutettu**, yritys voi todeta ja osoittaa, että kysyttävä asia on osittain kunnossa, mutta se vaatii edelleen kehittämistä
- **ei toteutettu**, kysyttävä asia on joko kokonaan hoitamatta tai vaatii vielä merkittävästi kehittämistä
- **ei koske meitä**, yritys voi osoittaa, että kysyttävä asia tai vaatimus ei koske sitä

Lisäksi jokaisen osion lopussa on ns. vapaa sana - kysymys.

Tuotamme vastausten perusteella raportin, jossa kuvataan yritysten strategisen tason menettelyjä digi- ja kyberturvallisuudesta. Raportti on tarkoitettu projektin sisäiseen käyttöön.

Haastattelupyyntö: Jos yritys niin haluaa, teemme mielellämme Teidän kanssanne täydentävän haastattelun, jossa tarkennamme digi- ja kyberturvallisuuteen liittyviä yrityksen toimintamalleja, osaamista ja resurssointia. Vastaukset haastattelupyyntöön tulee lähettää yhteyshenkilöille 16.9. mennessä.

Digipoolissa asiaa hoitaa Antti Nyqvist (antti.nyqvist@teknologiateollisuus.fi, +358408619446) toimittajan puolesta projektipäällikkö Pertti Kuokkanen (pertti.kuokkanen@cyberwatchfinland.fi).

Taustatiedot

1. Yrityksen nimi (vapaaehtoinen)

2. Yrityksen Y-tunnus (vapaaehtoinen)

3. Kyselyn yhteyshenkilö (sähköpostiosoite) (vapaaehtoinen)

4. Yrityksen toimiala (pakollinen)

   Elintarvikeala
   Energia-ala
   Finanssiala
   ICT- ja ohjelmistoala
   Kaupan- ja jakelun ala
   Logistiikka-ala
   Media-ala
   Satama- ja merenkulkualat
   Teleliikenneala
   Teollisuusala
   Terveydenhuoltoala
   Vesihuoltoala

5. Mikä on yrityksen koko henkilöstön ja/tai liikevaihdon määrän mukaisesti? (pakollinen)
   > 2000 konserni (>400 M€/v)
   > 250 suuryritys (> 50 M€/v)
   < 250 PK-yritys (< 50 M€/v)
   < 50 pienyritys (< 10 M€/v)
   < 10 mikroyritys (< 2 M€/v)

6. Kuinka paljon ovat olleet digitaalisen turvallisuuden kehittämis- ja ylläpitokustannukset vuonna 2020, arviotarkkuus riittää?
   0 euroa
   < 1000 euroa
   < 10 000 euroa
   < 100 000 euroa
   < 1 000 000 euroa
   > miljoona euroa

7. Mikä on yrityksen käyttämä henkilötyövuosimäärä (htv) omien ja ulkoisten henkilöiden digiturvatehtäviin vuonna 2020 (riskienhallinta, jatkuvuus ja valmius, tietoturva, kyberturva, tietosuoja), arviotarkkuus riittää?
   ___ 0-1
   ___ 1-2
   ___ 3-5
   ___ 5-10
   ___ yli 10

8. Onko yrityksessä vähintään yksi päätoiminen/oto henkilö seuraavilla digiturvallisuuden osa-alueilla? (valitse kaikki sopivat vaihtoehdot)

   päätoiminen/oto

   __ / __ riskienhallinta
   __ / __ jatkuvuus ja varautuminen
   __ / __ tietoturvallisuus
   __ / __ tietosuoja
   __ / __ kyberturvallisuus

9. Kuinka monta tuntia digitaalisen turvallisuuden koulutusta yrityksen henkilöstö on keskimäärin saanut vuonna 2020 (tuntia/henkilö), arviotarkkuus riittää?

   ___ 0
   ___ 1-2
   ___ 3-5
   ___ 5-10
   ___ yli 10

Seuraavien osioiden vastausvaihtoehdot: ei koske meitä, ei toteutettu, osittain toteutettu, täysin toteutettu (ellei toisin mainita)

Yrityksen strategiantyön lähtökohdat (painopiste)

1. Yrityksen arvot sisältävät digitaalisen turvallisuuden tekijät (Digitaalinen turvallisuus käsittää viisi osa-aluetta: riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvallisuuden, kyberturvallisuuden sekä tietosuojan.).

2. Yrityksen tuotanto- ja palvelutoiminnalle on asetettu tehokkuustavoitteet.

3. Yrityksen tuottamille tuotteille ja palveluille on asetettu digiturvallisuustavoitteet. (Digitaalisen turvallisuuden tavoitteena on suojata yrityksen toiminta niiltä riskeiltä ja uhkilta, jotka voivat kohdistua yrityksen henkilötietoihin ja tuotteisiin sekä prosesseihin, palveluihin ja tietoaineistoihin digitalisoituneessa toimintaympäristössä.)

4. Strategiatyössä on menettely, jolla voidaan tunnistaa yrityksen digitalisaatioon liittyvät mahdollisuudet.

5. Digiturvallisuudelle on asetettu taloudelliset tavoitteet.

6. Yrityksellä on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi.

7. Yritys käyttää standardoitua tai muuta vastaavaa menettelyä strategiatyön lähtökohtana.

8. Yrityksellä on kyky arvioida riittävä resurssointi ja budjetti digi- ja kyberturvallisuuteen.

9. Yrityksellä on riittävästi osaavaa henkilöstöä kyberturvallisuuden eri osa-alueilla.

10. Yrityksellä on riittävät resurssit ja osaaminen digitaalisen turvallisuuden ylläpitoon ja kehittämiseen osana yrityksen prosesseja, toimintamalleja ja järjestelmiä (kokonaisarkkitehtuuria).

11. Yrityksen on tunnistanut sen liiketoiminnan kannalta kriittiset toiminnot, palvelut, tiedot, tietovarannot ja tietojärjestelmät.

    a. Jos kyllä, niin miten ne ovat vaikuttaneet esimerkiksi alihankintaketjuihin? <vapaa laatikko>

12. Kyberturvallisuudelle on määritetty tehokkuusvaatimukset (kustannus-vaikuttavuus).

    a. Jos kyllä, niin anna toteutuksesta lyhyt digi- ja kyberturvallisuusesimerkki <vapaa laatikko>

13. Kuinka suuri osa yrityksen liiketoiminnasta on riippuvainen järjestelmien ja datan toimivuudesta ja digitaalisen tiedon eheydestä?

    ___ <20 %
    ___ 20-40 %
    ___ 40-60 %
    ___ 60-80 %
    ___ > 80 %

14. Yritys hyödyntää kyberturvallisuuskatsauksia (tilannekuva) strategisessa suunnittelussa.

15. **Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?**
(avoin vastaustila)

Yrityksen strategiatyö

1. Yrityksellä on säännöllinen ja toimiva strategiaprosessi tai toimintamalli yrityksen strategian (tai vastaavan tason ohjauksen) laatimiseen.

2. Yrityksen strategian (tai vastaavan) laatimisesta vastaa

    a. hallituksen puheenjohtaja / hallitus
    b. toimitusjohtaja / johtoryhmä
    c. strategiapäällikkö (vast)
    d. ei kukaan

3. Strategian (tai mission) perusteella yrityksen digitalisaatio liittyy (valitse tarvittaessa useampi)

    a. alustatalouteen (verkkokauppaan)
    b. hallintopalvelut (taloushallinto, henkilöstöhallinto)
    c. viestintään ja etätyöhön (sosiaalinen media, verkkokokoukset, etäjohtaminen)
    d. pilvipalveluihin (hajautetut järjestelmät)
    e. yrityksen operatiiviseen toimintaan
    f. toimitusketjuihin (liiketoimintamallit)
    g. yrityksen tuotteisiin ja palveluihin

4. Strategiatyössä on asetettu tavoitteet yrityksen

    a. taloudelle
    b. tuotteille ja palveluille
    c. tuotantotoiminnalle
    d. henkilöstön osaamiselle
    e. digitalisaatioasteelle
    f. toiminnan jatkuvuudelle (resilienssi)

    g. Jos johonkin em kyllä, niin millaisia tavoitteita on asetettu? <vapaa laatikko>

5. Yrityksen strategiassa (tai vastaavassa) on asetettu tavoitteet turvallisuuden osatekijöille:

    a. yleiset vaatimukset
    b. henkilöstöturvallisuus
    c. tilaturvallisuus
    d. työturvallisuus
    e. tietoturvallisuus
    f. kyberturvallisuus

    g. Jos johonkin em kyllä, niin millaisia tavoitteita on asetettu? <vapaa laatikko>

6. Yrityksen liiketoimintastrategiassa on määritetty digitaaliset menestystekijät.

    a. Jos kyllä, niin millaisia menestystekijöitä on määritetty? <vapaa laatikko>

7. Yrityksen johto on sitoutunut digitaalisen turvallisuuden kehittämiseen.

8. Strategiatyössä on menettely, jolla voidaan tunnistaa yrityksen digitalisaatioon liittyvät uhkatekijät.

9. Strategiatyössä on määritelty viestinnän linjaukset ja avoimuusperiaatteet mahdollisen kriisitilanteen varalta.

10. **Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?**
(avoin vastaustila)

Yrityksen strategian toimeenpano ja tulosten mittaaminen

1. Yrityksen digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia.

2. Yrityksellä on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja.

3. Yrityksellä on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.

4. Yrityksellä on menettely, jolla se seuraa toimintaympäristössä tapahtuvia ilmiöitä ja arvioi niiden vaikutusta yrityksen toimintaan.

5. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa, (toimitusketjun hallinta).

6. Yrityksellä on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn.

7. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti yrityksen johdolle.

8. Yrityksessä viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko yrityksen laajuisesti.

9. Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti.

10. Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta ja henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta.

11. Yritys harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista.

12. Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella.

13. **Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?**

    (avoin vastaustila)

Yrityksen digi- ja kyberturvallisuustoimenpiteiden nykytilanne

1. Yrityksen tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi.

2. Yrityksellä on strategiaprosessi, joka huomioi kyberympäristön vaikutukset omaan liiketoimintastrategiaan.

    a. Anna toteutuksesta esimerkki <vapaa laatikko>

3. Yritys on huomioinut digitaalisen turvallisuuden osana yrityksen prosesseja, toimintamalleja ja järjestelmiä (kokonaisarkkitehtuuria).

4. Yritys tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt (kyberturvallisuus), toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.

5. Yritys on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet.

6. Yritys on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.

7. Yrityksessä on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten yritysten tai yhteiskunnan toimintaan.

8. Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia.

9. Yrityksessä on määritelty digitaaliseen turvallisuuteen liittyvät mittarit, joiden avulla yritys voi seurata osa-alueiden kehittymistä.

10. Yrityksessä kehitetään riskienhallintaprosessia riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella.

11. Yrityksellä on kyky valita toiminnan edellyttämät kyberturvalliset teknologiat.

12. Yrityksen tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa.

13. Yrityksellä on toteuttamiskelpoinen varautumisen ja jatkuvuuden hallinnan suunnitelma.

    a. Jos kyllä, niin anna toteutuksesta lyhyt digi- ja kyberturvallisuusesimerkki <vapaa laatikko>

14. Yrityksellä on häiriö- ja kriisitilanteiden viestintäsuunnitelma.

15. Yrityksessä tietoturvasta ja tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi.

16. Kuinka moneen digitaaliseen turvallisuuteen liittyvään harjoitukseen yritys on osallistunut vuoden 2020 aikana?

    ___ 0
    ___ 1–2
    ___ 3-5
    ___ yli 5

17. Kuinka monta digitaaliseen turvallisuuteen liittyvää harjoitusta **yritys on itse järjestänyt** vuoden 2020 aikana?
    ___ 0
    ___ 1-2
    ___ 3-5
    ___ yli 5

18. **Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?**
    (avoin vastaustila)