KYBERTURVALLISUUDEN NYKYTILA ERI TOIMIALOILLA – KARTOITUKSEN KESKEISET HAVAINNOT

HUOLTOVARMUUSORGANISAATIO

KYBERTURVALLISUUDEN NYKYTILA ERI TOIMIALOILLA – KARTOITUKSEN KESKEISET HAVAINNOT

www.huoltovarmuus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Julkaisija:
Huoltovarmuusorganisaation Digipooli

Tiivistelmän tekijä:
Huoltovarmuuskeskus yhteistyössä Digipoolin ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kanssa. Pohjautuu Digipoolin teettämään selvitykseen, jonka teki KPMG.

Kuvat: Shutterstock

Taitto: Up-to-Point Oy

Julkaisuvuosi: 2020

ISBN: 978-952-5608-79-3

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

Sisältö

1 JOHDANTO

Kyberturvallisuuden merkitys huoltovarmuudelle lisääntyy, kun yhteiskunnan kriittiset yritykset digitalisoivat keskeisiä toimintojaan. Sen seurauksena digitaaliset ympäristöt ja yhteydet eivät enää vain tue yritysten liiketoimintaa, vaan ovat välttämättömiä toiminnalle. Huoltovarmuusnäkökulmasta yritysten digitaaliseen turvallisuuteen tulee kiinnittää huomiota samassa suhteessa kuin sen merkitys kasvaa osana liiketoiminnan edellytyksiä.

Kyberturvallisuutta edistävien toimenpiteiden kohdentaminen ja vaikutusten seuranta on ollut hankalaa vertailukelpoisen tiedon puutteessa. Huoltovarmuusorganisaation Digipooli tarttui haasteeseen ja toteutti kyberturvallisuuden nykytilasta kattavan selvityksen, joka käsitti 12 toimialaa ja yli 100 yritystä. Kartoitus sisälsi 30 kysymystä, joiden avulla on saatu yritysten liiketoimintajohdon näkökulma nykytilanteesta kyberturvallisuuden johtamiseen ja ohjaamiseen Suomessa. Tuloksena saatiin kehityskohteita yritysten, toimialojen ja niiden riippuvuuksien väliseen kyberturvallisuuteen.

Merkittävin pitkäaikainen vaikutus organisaation kyberturvallisuuden myönteiseen kehittymiseen toteutuu, kun ylin johto sitoutuu ja ohjaa asettamalla kyberturvallisuuden tavoitteet ja vastuut. Silloin kyberturvallisuuden kehittäminen on todennäköisesti systemaattista ja riskiperusteista eikä riippuvaista yksittäisten kyberturvallisuusasiantuntijoiden osaamisesta ja innokkuudesta. Selvityksessä on mitattu juuri mainittujen perusasioiden johdonmukaista toteutumista.

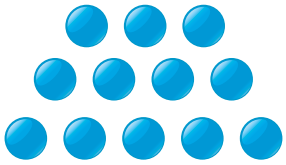
Tämä tiivistelmä kokoaa yhteen keskeiset kehityskohteet ja päähavainnot valmistuneiden raporttien tuloksista. Yritykset ovat vastaanottaneet omat ja toimialakohtaiset tulokset. Lisäksi toimialakohtaisia tuloksia jaetaan toiminnan kehityksestä vastaaville tahoille kuten poolien käyttöön.

Ydinhavainto on, että kaikkien toimialojen tilanne on keskimäärin vähintään kohtalainen, mutta yritysten välillä on laajaa hajontaa. Huoltovarmuusnäkökulmasta on olennaista tasata eroja, jotta riippuvuusverkostot ovat kauttaaltaan kyberiskun kestäviä. Tähän nykyinen taso antaa hyvät lähtökohdat. Tulokset ovat myös keskeistä pohjatietoa, kun valitaan projekteja valmisteilla olevaan Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelmaan vuosille 2020-2025.

Digipoolin toimeksiannosta KPMG:n kyberturvallisuuskonsultit toteuttivat selvityksen talvella 2019-2020. Tuloksena saatiin määritettyä toimialojen kyberturvallisuuksille lähtötasot. Selvitys on tarkoitus toteuttaa säännöllisesti noin kahden-kolmen vuoden välein käynnistettyjen kehitystoimenpiteiden vaikutusten ja yleisten trendien seuraamiseksi.

2 TULOSTEN TIIVISTELMÄ

Tutkimuksen laajuus



- 100 + organisaatiota
- 12 toimialaa

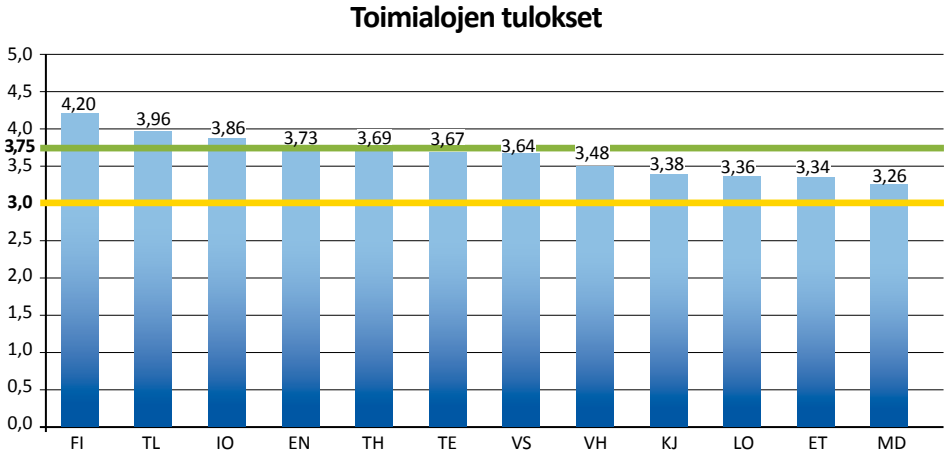
Arviointiasteikko

5 Kehitetään jatkuvasti riskilähtöisesti
4 Tehdään johdonmukaisesti
3 Määritetty tai suunniteltu
2 Tehdään vaihtelevasti ja/tai osittain
1 Ei tiedä

Tavoitteet

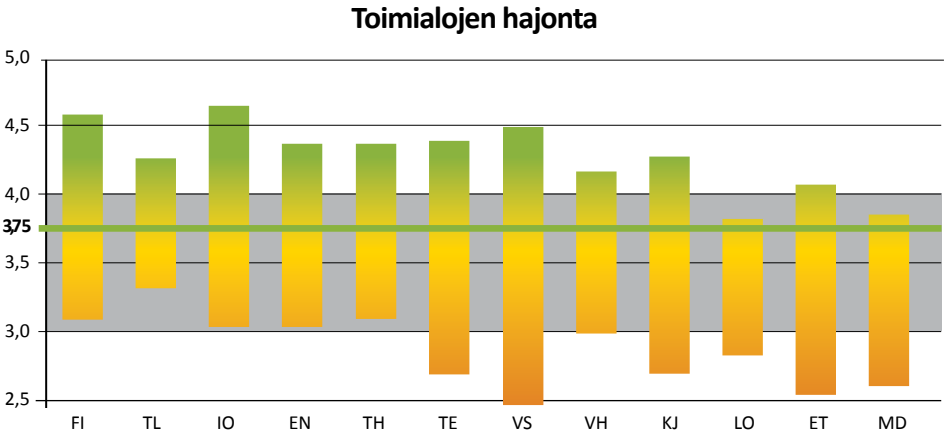
4 **Organisaation riski laskee**

3,75 **Toimiala tukee muita**



FI= finanssiala, TL= teleliikenneala, IO= ICT- ja ohjelmistoala, EN= energia-ala, TH= terveydenhuoltoala, TE= teollisuusala, VS= satama- ja merenkulkualat, VH= vesihuoltoala, KJ= kaupan- ja jakelun ala, LO= logistiikka-ala, ET= elintarvikeala, MD= media-ala

Kuva 1. Kaikki toimialat ylittivät arvion keskinkertainen.



FI= finanssiala, TL= teleliikenneala, IO= ICT- ja ohjelmistoala, EN= energia-ala, TH= terveydenhuoltoala, TE= teollisuusala, VS= satama- ja merenkulkualat, VH= vesihuoltoala, KJ= kaupan- ja jakelun ala, LO= logistiikka-ala, ET= elintarvikeala, MD= media-ala

Kuva 2. Hajonta on laajaa useilla toimialoilla yritysten välillä.

KEHITYSKOHTEET

Merkittävimmät yhteiset huoltovarmuusnäkökulmasta

1. Yhteinen tilannekuva
2. Turvallinen ohjelmistokehitys
3. Henkilöstön osaaminen

Tärkeimmät yhtenevät yritysten liiketoiminnan näkökulmasta

1. Yrityksen kyberturvallisuus-strategia
2. Kyberturvallisuusarkkitehtuuri
3. Tekninen jäljitettävyys

Lisäksi toimialakohtaisia kehitystarpeita, jotka edesauttavat toimialan lisäksi turvallisuutta toimialojen välisissä riippuvuuksissa.

JOHTOPÄÄTÖKSIÄ TULOKSISTA

Aiheuttavat haastetta

1. Toimialojen välisten riippuvuuksien ymmärrys tärkeää huoltovarmuudessa
2. Kyberturvallisuuden ohjaaminen siiloutuu usein kokonaisuudesta erillisiin osastoihin
3. Perusasioissa edelleen kehitettävää

Tukevat kehitystä

4. Hajonta mahdollistaa yhteistyön
5. Reaktiivisessa toiminnassa parhaat kypsyystasot
6. Yritykset tunnistavat kyberturvallisuuden hankintaketjussa sopimusperusteisesti
7. Sääntely vaikuttaa myönteisesti turvallisuuden edistämiseen

Huomioitavaa:

Tulokset kuvaavat yritysten liiketoimintajohdolle kyberturvallisuuden prosessien ja menetelmien kypsyyttä organisaatioissa johtamisen ja ohjaamisen tueksi. Tulokset eivät suoraan kerro teknisen kyberturvallisuuden tasosta ja toteutuksesta yrityksissä, mitkä voivat osaavan kyberhenkilöstön tai palveluntarjoajan toteuttamana poiketa selvityksen tuloksista. Oletettavaa kuitenkin on, että pääsääntöisesti kyberturvallisuus kehittyy parhaiten, kun johto on sitoutunut ja ohjaa toimintaa – johdetut tavoitteet vastaavat käytännön toteutusta.

3 MERKITTÄVIMMÄT KEHITYSKOHTEET

Selvityksellä löydettiin useita toimialoja poikkileikkaavia kehityskohteita, jotka toistuivat tuloksissa käytettäessä erilaisia arviointitapoja: liiketoimintariskilähtöinen, riskipainotteinen ja toimialojen väliset riippuvuudet. Merkittävimpiä kehityskohteita arvioitaessa on painotettu yritysten liiketoimintariskinäkökulmaa, koska katsottiin, että se on yritysten ja elinkeinoelämän toimivuuden kannalta vaikutuksiltaan merkityksellisin huoltovarmuudelle. Kartoituksen merkittävin arvo on laajan yhdenmukaisen arvioinnin avulla esiin nostetut kehityskohteet.

Alla olevassa kuvassa kehityskohteet on jaettu kahteen kategoriaan sen mukaan, toteutuuko tavoite ensisijaisesti yrityskohtaisesti vai yhteisesti huoltovarmuuslähtöisesti.

Yrityskohtaisesti merkittävät useille yhtenevät kehityskohteet:

1. Yrityksen kyberturvallisuusstrategia (3.1)
2. Kyberturvallisuusarkkitehtuuri (3.2)
3. Tekninen jäljitettävyys (3.3.)

Huoltovarmuuden kannalta merkittävät yhteiset kehityskohteet:

1. Yhteinen tilannekuva (3.4)
2. Turvallinen ohjelmistokehitys (3.5)
3. Henkilöstön osaaminen (3.6)

Yrityskohtaisesti tärkeimmät kehityskohteet voivat vaihdella suuresti, koska tuloksissa oli runsaasti hajontaa. Tyypillisesti tuloksia heikensi, jos asia pyrittiin osoittamaan käytännössä toteutetuksi dokumentoinnin puutteesta huolimatta. Tällaisissa tapauksissa katsottiin, että selkeä johdon strateginen linjaus tavoitteineen puuttui. Toimialalle tyypilliset erityispiirteet ja digitalisaation kehitysvaiheet ovat taustalla monissa toimialatulosten eroissa. Toimialakohtaisten tulosten pääkohdat löytyvät luvusta 5 ja liitteistä. Seuraavaksi tarkastellaan suurelle osalle yhteneviä pääkehityskohteita.

3.1 Yrityksen kyberturvallisuusstrategian suunnittelu

Selite: Yrityksen kyberturvallisuusstrategia on kyberturvallisuuden kehityksen perusta. Yksinkertaisimmillaan yrityksen kyberturvallisuusstrategiassa on kyberturvallisuuden tavoitteet ja suunnitelma niiden saavuttamiseksi. Korkeammalla kypsyystasolla yrityksen kyberturvallisuusstrategia sisältää myös prioriteetit, hallintamallin kuvauksen, kyberturvallisuuden hallintaorganisaation rakenteen ja vastuut sekä ylimmän johdon sitoutumisen ja osallistumisen hallinnan suunnitteluun ja järjestämiseen.

Useiden toimialojen yrityksiltä puuttuu riittävä riskienhallintastrategia, kyberturvallissuustrategia tai kyberturvallisuusriskien hallinta. Silloin kyberturvallisuus nähdään ensisijaisesti teknisenä tukitoimena sen sijaan, että kyberturvallisuus nähtäisi pitkäjänteisesti kehitettynä ja riskit hallittuna tukevan yrityksen liiketoimintaa. Jotta yritys voi siirtyä tietotekniikkaa tehokkaasti hyödyntävään toimintamalliin, sen tulee määrittää kyberturvallisuuden tavoitetila ja sen toteuttamiseksi strategia.

Tämä voi tapahtua esimerkiksi osana liiketoiminnan riskien hallintaa tai turvallisuuden suunnittelua. Muuten lisääntyvät it-riippuvuudet kasvattavat niiden toimivuudesta riippuvaisten toimintojen liiketoimintariskejä merkittävästi. Näin uhkiin reagoimisen sijaan päästään toimintaa tukevaan ja eteenpäin vievään malliin.

On hyvä huomioida, että strategiaksi riittää esimerkiksi lyhytkin dokumentti, joka pitkällä aikavälillä ohjaa kyberturvallisuudesta vastaavia henkilöitä turvallisuuden kehittämisessä, valinnoissa ja investoinneissa. Näin päätöksentekijät saavat visionsa mukaisia ehdotuksia kehitystoimista.

Yrityksen kyberturvallisuuden strategian laatiminen ja sen pohjalta kyberturvallisuusriskien hallinta on kehitystoimena jokaisen yrityksen omalla vastuulla. Jotta sen toteutuminen edistyisi yrityksissä, voi yrityksen kyberturvallisuusstrategian laatimiseen tehdä asiaa helpottavaa ohjeistusta ja käytäntöjä.

3.2 Kyberturvallisuusarkkitehtuuri

Selite: Kyberturvallisuusarkkitehtuuri on olennainen osa yrityksen tietojärjestelmien kokonaisarkkitehtuuria. Sen avulla kuvataan organisaation turvallisuusprosessien, kyberturvallisuusjärjestelmien ja henkilöstön rakenne sekä näiden suhde organisaation tavoitteeseen ja strategisiin suunnitelmiin. Tärkeä osa kyberturvallisuusstrategiaa on IT- ja OT-ympäristöjen onnistunut eriyttäminen.

Selvityksen perusteella vain harva yritys käsittelee tällä hetkellä kyberturvallisuusarkkitehtuuria yrityksen it-järjestelmien kokonaisarkkitehtuurin osana. Lisäksi arkkitehtuurin taso on kirjava. IT- ja OT-ympäristöjen (information technology, operational technology) turvallisuuden hallinnan tulisi olla arkinen osa kokonaisuutta ja toteuttaa yrityksen kyberstrategiaa, eikä olla jälkikäteen rakennettua suojausta ja havainnointia digitaalisten toteutusten ympärille. Myönteistä oli, että osassa organisaatioita näin tämä olikin toteutettu, mutta useimmilla se oli vasta ajatuksena valmisteilla tai sen käynnistämiseen tarvittaisiin ulkopuolista tukea. Valtaosa organisaatioista kertoo, että johto tukee vahvasti kyberturvallisuusarkkitehtuurin ylläpitämistä ja kehittämistä, mutta se ei vielä ole osa toimintaa.

Jokaisen organisaation kyberturvallisuusarkkitehtuuri on yksilöllinen ja vaatii yrityskohtaisen toteutuksen. Huoltovarmuuden kehittämiseksi yrityksiä voi parhaiten tukea käytäntöjen laatimisessa ja toteutettujen ratkaisujen arviointikäytännöissä.

3.3 Tekninen jäljitettävyys

Selite: Suojattavien kohteiden tila (tunnistettuna seurannan kautta) vaikuttaa operatiiviseen tilannekuvaan. Parhaimmillaan kriittisten järjestelmien lokeja kerätään systemaattisesti keskitettyyn lokien hallintajärjestelmään jatkuvaa valvontaa varten ja lokien valvonnassa on otettu huomioon organisaation uhkaprofiilit ja riskit.

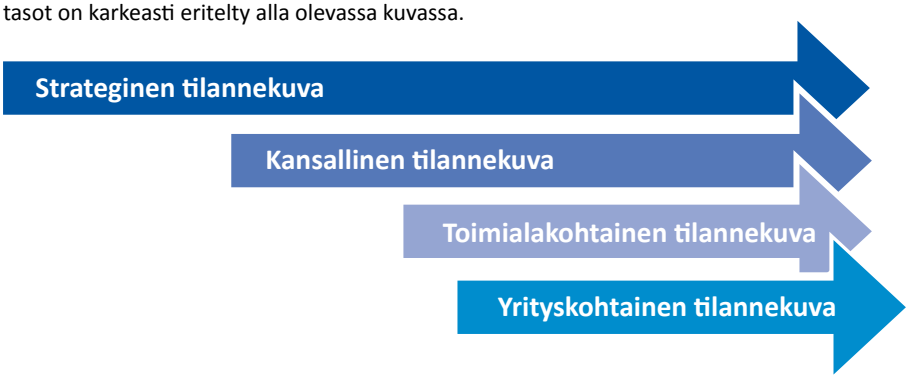
Tekninen jäljitettävyys eli lokien seuranta on itsessään tärkeä kyberturvallisuutta edistävä toimenpide, mutta myös pohja monille muille toimenpiteille. Lokit tukevat tilanneymmärrystä ja poikkeamien sattuessa ovat olennainen osa onnistuneita korjaustoimenpiteitä ja nopeata palautumista. Tekninen jäljitettävyys toimii näin myös havaittujen ongelmien korjaamisessa kehitystyön tukena. Parhaisiin käytäntöihin perustuva lokituspolitiikka, eli tarpeeksi kattava lokitus ja sitä tukeva suojattavien kohteiden hallinnoiminen (asset management), on yksi perusperiaate hyvälle ja ajantasaiselle tilannekuvan muodostamiselle (3.4). Tulokset kuitenkin osoittavat, että lokittamisessa on vielä useilla toimijoilla kehittämisen varaa.

Lokituksen toteutus on yrityskohtainen toimenpide, johon löytyy markkinoilta runsaasti ratkaisuja ja ohjeita oikeaoppisesta toteutuksesta, eli helposti toteutettava. Huoltovarmuuden parantamiseksi on etsittävä keinoja, joilla lokitus otetaan kattavasti käyttöön yritysten verkoissa ja järjestelmissä, jotta asia etenee yrityksissä käytännön toteutukseen kyberturvallisuuden ylläpitämisen tueksi.

3.4 Tilannekuvan kehittäminen

Selite: Yhteisen operatiivisen tilannekuvan ydin on operatiivisen kuvan kommunikointi keskeisille päätöksentekijöille ja sidosryhmäverkostolle. Useat yhteisen operatiivisen tilannekuvan toteutukset saattavat sisältää visuaalisia elementtejä (esim. hallintapaneelit, kartat tai muut graafiset käyttöliittymät), mutta ne eivät ole pakollisia tavoitteiden saavuttamiseksi. Organisaatiot voivat myös käyttää muita tapoja tilannekuvan viestimiseen.

Tilannekuvan päätavoite on saada kyberturvallisuutta tukeva tilanneymmärrys. Yhtenäisen tilannekuvan tarve toistui niin yritysten kuin toimialojen tuloksissa. Tilannekuva on varsin laaja käsite, jonka alta on tunnistettavissa eri osa-alueita, joiden nykyinen kypsyystaso vaihtelee suuresti. Nämä tasot on karkeasti eritelty alla olevassa kuvassa.



Kuva 3. Tarvitaan tilannekuvaa monella tasolla yhteisen tilanneymmärryksen saamiseksi.

Yritysjohdolle strateginen tilannekuva kertoo tulevaisuuden kehityssuunnista. Se muodostaa tarpeellisen tuen, kun määritetään strategiaa ja sen mukaisia investointeja liiketoiminnan tueksi. Tästä syystä huoltovarmuusnäkökulmasta on tärkeää, että kehitetään yhteisesti hyödynnettävä kyberturvallisuuden strateginen tilannekuva.

Kansallisen tilannekuvan muodostamiseksi on tehty runsaasti kehitystoimenpiteitä vuosien aikana. Esimerkiksi on perustettu Kyberturvallisuuskeskus ja sitä kautta erilaisia tilannekuvatuotteita ja ISAC-tiedonvaihtoverkostoja. Yritysten ja viranomaisten välistä yhteistyötä on lisätty, ja sitä on tulosten perusteella syytä jatkaa ja jatkokehittää.

Lisäksi yrityksillä on tarvetta toimialakohtaiselle operatiiviselle tilannekuvalle. Sen toteuttamista edesauttaa yhteinen kehitystoiminta, jossa yritykset ovat vahvasti sitoutuneena mukana. Tähän kehitykseen on syytä panostaa hyödyntämällä jo olemassa olevia verkostorakenteita, erityisesti ISAC-verkostot.

On myös tarve yrityskohtaiselle tilannekuvalle, joka on lähtökohtaisesti yritysten sisäistä kehitystoimintaa. Yrityskohtainen tilannekuva palvelee kunkin organisaation järjestelmien kyberturvallisuuden ylläpitämistä yrityskohtaisten laite- ja ohjelmistovalintojen osalta ja suhteessa toiminnan riippuvuusketjussa oleviin organisaatioihin. Sen tukemiseksi on mahdollista laatia parhaita käytäntöjä, jotka edesauttavat laajasti useita huoltovarmuuskriittisiä yrityksiä määrittämään esimerkkien kautta tilannekuvasisällön, joka tukee omaa toimintaa. Edellä mainitut toimialakohtainen ja kansallinen tilannekuva tukevat sisällöllisesti yrityskohtaista tilannekuvaa.

3.5 Turvallinen ohjelmistokehitys

Selite: On tärkeää noudattaa ja edellyttää turvallista ohjelmistokehitystä, kun kehitetään suojattavia kohteita sisältäviä ohjelmistoja. Tämä pienentää merkittävästi mahdollisten haavoittuvuuksien synnyn todennäköisyyttä.

Turvallinen ohjelmistokehitys on mainittu kaikkien toimialojen kehityskohdelistalla ja nousi useiden toimialojen tuloksissa tärkeimmäksi kehityskohteeksi. Erityisen merkitykselliseksi se nousee toimialoilla, joilla käytettävien järjestelmien elinkaari on tyypillisesti pitkä, kuten energiantuotanto ja vesihuolto.

Kyberriskit realisoituvat käytännössä ohjelmistojen kautta. Turvallinen ohjelmistokehitys pienentää uhkien realisoitumista, ohjaa henkilöstöä käyttämään ohjelmistoja ja sovelluksia turvallisesti ja pienentää virheiden vaikutuksia. Ohjelmistoturvallisuus tulisi huomioida aina hankinnasta elinkaaren loppuun saakka ja käytöstä poistamiseen. Pitkien elinkaarten järjestelmien ohjelmistoheikkoudet ovat erityisen riskialttiita, koska ohjelmistojen päivittäminen ja ylläpitäminen on kallista. Lisäksi ajan kuluessa riskiksi nousee ohjelmistovalmistajan toiminnan jatkuvuus. Ohjelmistojen turvallisuus pitäisi huomioida valmisohjelmistojen hankintojen lisäksi räätälöidyissä ohjelmistoissa, itse tehdyissä ohjelmistoissa ja koodinpätkissä niin organisaation omissa ympäristöissä kuin pilvipalveluissa.

Ohjelmistojen turvallisuuden huomiointi on ennen kaikkea yhteinen kehityskohde. Yhteinen tarve lähtee laajalle levinneestä asenteesta huomioida kyberturvallisuus ja jatkuvuuden hallinta osana ohjelmistokehitystä alusta saakka. Se toteutuu järjestelmällisesti, kun ohjelmistovalmistajien työntekijöille on koulutettu riittävä osaaminen tehdä ja tarjota turvallista ohjelmistokehitystä. Toisesta näkökulmasta myös yritysten täytyy ostajina osata vaatia turvallisuutta osana ohjelmistohankintoja ja -sopimuksia. Kansallisesti olisi hyödyllistä ottaa käyttöön esimerkiksi yhteisiä suosituksia minivaatimuksista ohjelmistojen turvallisuudelle, kuten kuluttajalaitepuolella Kyberturvallisuuskeskuksen tietoturvamerkki on tuonut.

3.6 Henkilöstön kehittäminen

Selite: Kyberturvallisuuskulttuurin ylläpitämiseksi kannattaa suunnitella ja toteuttaa toimenpiteitä, prosesseja ja teknologioita sekä kouluttaa henkilöstöä, jotta asenne ja osaaminen kasvaa – huomioiden riskit organisaation tavoitteiden ja kriittisen infrastruktuurin osalta.

Henkilöstön kyberturvallisuusosaaminen nousee tuloksissa esille useasta eri näkökulmasta. Yksi näkökulma on koko henkilöstön perusosaaminen, toinen kyberturvallisuusasiantuntijoiden toimialakohtaisen osaamisen ylläpitäminen ja kolmas henkilöstön työsuhteen elinkaaren hallinta. Kaikki edellä mainitut näkökulmat ovat tärkeitä.

Henkilöstön kyberturvallisuusosaamista olisi syytä lisätä etenkin toimialoilla, jossa se ei kuulu ydinosaamiseen tai henkilöstön vaihtuvuus on suurta kuten kaupan ja jakelun alalla. Tämän lisäksi on hyvä kiinnittää huomiota erikoisosaamista vaativien alojen henkilöstön kyberturvallisuusosaamiseen, kuten prosessiteollisuus, vesihuolto tai energiantuotanto.

Kyberturvallisuushenkilöstön kehittämiseen kuuluu rekrytointien ja koulutuksen kautta tunnistettujen osaamispuutteiden paikkaaminen. Esimerkiksi, rekrytointitoimenpiteiden tulisi varmistaa, että rekrytoivat henkilöt ja haastateltavat ovat tietoisia kyberturvallisuushenkilöstön tarpeista. Tähän kuuluu myös ymmärrys turvallisuusselvityksistä. Lisäksi, uusien henkilöiden (ja ohjelmisto- ja palvelutoimittajien) tulisi suorittaa kyberturvallisuuskoulutus, jotta heidän alttiuttaan sosiaaliselle hakkeroinnille ja muille uhkille voidaan pienentää.

Työntekijät vaihtuvat eri yritysten välillä ja monet henkilöstön perusosaamistarpeet toistuvat samanlaisina läpi yritysten ja toimialojen. Tästä syystä aiheesta on löydettävissä runsaasti yhteisiä, kaikkia hyödyttäviä kehityskohteita, jotka toteutuessaan edistävät kyberturvallisuutta laajasti huoltovarmuuskriittisissä yrityksissä.

4 JOHTOPÄÄTÖKSIÄ KYBERTURVALLISUUDEN EDISTYMISESTÄ

Kartoituksen tuloksista välittyy käsitys, että kyselyyn valituilla organisaatioilla on erittäin hyvä ymmärrys tärkeästä asemastaan tuottaa yhteiskunnallisesti elintärkeitä tuotteita ja palveluita. Tämä edesauttaa yhteisten kehitystoimenpiteiden tekemistä.

Nyt saaduista tuloksista hahmottuu, mitkä aiemmin toteutetut toimenpiteet ovat johtaneet kyberturvallisuuden edistymiseen tietyillä toimialoilla tai osa-alueilla. Toisaalta esiin nousee myös, missä asioissa tarvitaan kokonaisvaltaisesti lisää ymmärrystä, jotta kyetään laajasti edistämään kyberturvallisuutta.

Yksi yleinen havainto on, että erittäin monissa organisaatioissa kyberturvallisuusasioita ei käsitellä ylimmässä johdossa. Ensi alkuun johdon tueksi sopii esimerkiksi Kyberturvallisuuskeskuksen laatima Kyberturvallisuus ja yrityksen hallituksen vastuu -opas. Kulttuurinen muutos on myös edellytys monien kehitystoimenpiteiden jalkautukselle käytäntöön ja siten avain kyberturvallisuuden kansalliseen kehitykseen, mikä edistää myös digitaalisen huoltovarmuuden toteutumista.

4.1 Toimialojen välisten riippuvuuksien ymmärrys

Yhteiskunnan elintärkeiden toimintojen turvaaminen ja huoltovarmuus muodostuvat riippuvuussuhteista rakentuvien ketjujen kautta. Huoltovarmuusnäkökulmasta nämä ketjut on syytä tunnistaa, jotta häiriöiden vaikutukset riippuvuusketjuissa kyetään minimoimaan. Kaikki selvityksessä olleet toimialat tunnistavat olevansa nykyisessä digitalisoituneessa toimintamallissaan riippuvaisia perusinfratoimialoista, joita ovat finanssi-, teleliikenne, ohjelmisto-, energia- ja teollisuustuotanto. Nämä toimialat muodostavat ytimen, jonka häiriöt heijastuvat nopeasti ja laajasti yhteiskuntaan.

Toimialojen välisiä riippuvuussuhteita voidaan yleistasolla tarkastella alla olevan kuvan kautta. Varsinaiset uhkat toteutuvat lopulta yksittäisten toimijoiden ja niiden käyttämien yksilöllisten järjestelmien välityksellä, eivät suoraan kuvan mukaisesti. Kuvan perusteella kuitenkin havaitaan, kuinka monimuotoisen ja keskinäisriippuvaisen verkoston toimialat keskenään muodostavat. Digitalisoitumisen edistyessä verkoston monimutkaistuminen jatkuu edelleen. Poikkeamien kestot näkyvät verkostossa eri tavalla: lyhyt minuuttien tai tuntien katkos on toimenpiteiltään ja vaikutuksiltaan erilainen kuin päivien tai viikkojen häiriö. Jatkuvuudenhallinnan toimenpiteitä suunniteltaessa on huomioitava nämä eri aikamääreet.

Toimialariippuvuudet

Kuva 4. ***Toimialariippuvuudet Kyberturvallisuus eri toimialoilla -kartoituksen mukaan vuonna 2020.***

Verkoston häiriöihin voi varautua esimerkiksi kahdella tyypillisellä tavalla:

1. ***parantamalla toimialan kyberturvallisuutta häiriösietoisemmaksi***, jolloin häiriöt eivät vaikuta merkittävästi toimintaan. Kyberympäristössä häiriösietoisuus tarkoittaa esimerkiksi vaihtoehtoisia yhteyksiä ja varajärjestelmiä.
2. ***ottamalla käyttöön vaihtoehtoisia toimintatapoja*** häiriön vaikutusten ajaksi. Tyypillinen esimerkki vaihtoehtoisesta toimintatavasta on varavoiman käyttö sähkökatkossa tai palaaminen manuaaliseen toimintaan ohjelmisto-ongelman ajaksi.

On huomioitava, että vaikka itse toimintakyky olisi olemassa, voivat sen ylläpitämiseksi tehdyt toimenpiteet heijastua muille toimialoille. Tästä tuoreimpana esimerkkinä on monille toimialoille sivuvaikutuksia aiheuttanut terveydenhuollon toimintakyvyn suojeleminen koronapandemian aikaan. Lyhyetkin toimintahäiriöt voivat vaikuttaa useiden alojen toimintaan. Tästä esimerkkinä vesihuolto: elintarviketeollisuus, sairaalat ja teollisuustuotannon laitokset voivat joutua keskeyttämään toimintansa jo muutaman minuutin vesikatkon johdosta, ellei veden saantia ole muilla tavoin tilapäisesti varmistettu.

Yksittäisen organisaation ja toimialan tärkeimmät asiakkaat verkostossa ovat usein toiset organisaatiot, joiden kautta vaikutukset heijastuvat yhteiskuntaan viranomaisille ja kansalaisille. Kokonaisuutta ei pysty kukaan 100-prosenttisesti hallitsemaan. Kukin organisaatio on tavallaan solmu, johon ja josta muodostuu muuttuvia yhteyksiä. Oman solmun kypsyyttä nostamalla parantaa koko verkoston toimintavarmuutta. Esimerkiksi ongelmat tietoliikenneyhteyksissä heijastuvat välittömästi muiden toimialojen arkeen, kun verkkoon ei pääse tai sähköpostin välityksessä on ongelmia. Samoin ohjelmisto-ongelma logistiikkayrityksessä voi aiheuttaa häiriöitä kuljetuksiin, mikä vaikuttaa tuotteiden ja varaosien saatavuuteen toisella toimialalla.

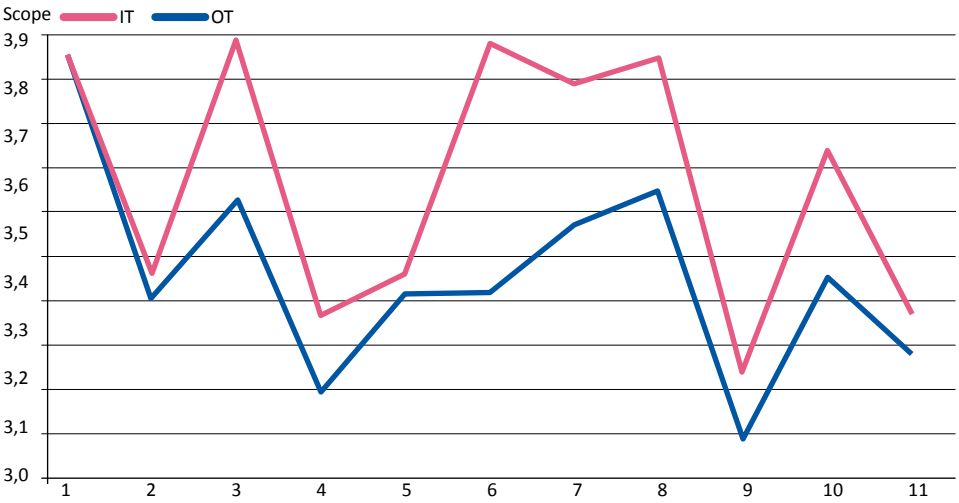
Edellä olevista syistä johtuen kehitystyössä on oman toiminnan lisäksi hyvä ottaa huomioon, miten oma toiminta on riippuvainen muista toimialoista tai miten oma toiminta vaikuttaa muihin aloihin – ja tehdä kyberturvallisuudessa yhteistyötä ja tiedonvaihtoa toimitusketjuissa muiden kanssa omaksi eduksi. Voi olla syytä harkita, että tiedonvaihto ja yhteinen varautuminen huomioidaan myös sopimuksissa.

4.2 Kyberturvallisuuden ohjaaminen ja jakautuminen kokonaisuudesta osastoihin (IT/OT)

Usein kyberturvallisuuden kokonaisuus jakautuu kahteen tai useampaan ympäristöön. Tyypillisesti näitä ovat:

- IT-ympäristö eli perinteinen toimistoverkko
- OT-ympäristö eli operatiivinen tuotantoympäristö

Kartoituksen perusteella näitä ohjataan ja hallitaan usein täysin erillisesti. Tämä on aiheuttanut useilla toimialoilla eroja ympäristöjen kyberturvallisuuden kypsyydessä yrityksen sisällä. Niinpä selvityksessä päädyttiin kirjaamaan IT- ja OT-ympäristöjen kypsyysarvioinnin tulokset erikseen kummallekin ympäristölle. Tulosten keskiarvot on kuvattu graafina sivulla 18. Verkottumisen myötä toiminta on harvoin täysin erillistä ja kokonaisuuden edistämistä tulisi hallita yhdenmukaisesti. Johdonmukaisesti tähän päästään laatimalla kokonaisuuden huomioiva kyberturvallisuusstrategia (3.1), jossa erilliset tarpeet ja turvallisuusympäristöt huomioidaan segmentoinnilla kyberarkkitehtuurin toteutuksessa (3.2)



1. Kriittisten palveluiden suojaaminen
2. Riskienhallinta
3. Suojattavien kohteiden, muutosten ja konfiguraatioiden hallinta
4. Kyberturvallisuuden hallintajärjestelmä
5. Toimitusketjun ja ulkoisten riippuvuuksien hallinta
6. Identiteettien, pääsyn- ja käyttövaltuuksien hallinta
7. Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus
8. Tiedonjako ja viestintä
9. Tilannekuva
10. Uhkien ja haavoittuvuuksien hallinta
11. Henkilöstöhallinto

Kuva 5. IT- ja OT-ympäristöjen kypsyysarviot.

4.3 Perusasioissa edelleen kehitettävää

Kartoituksen kautta saadut tulokset osoittavat, että monien perusasioiden järjestelmällinen toteuttaminen on edelleen kesken. Esimerkiksi tekninen jäljitettävyys (lokitus) ja pääsynhallinta (identiteetin hallinta) löytyvät useiden yritysten kehityskohteista, vaikka niiden ratkaisun tueksi on ollut vuosien ajan saatavissa oppaita ja laajasti teknisiä ratkaisuja.

Valitettavasti kyberturvallisuuden tason nostaminen onnistuu vasta, kun perusta on kattavasti hyvin toteutettu, mikä edellyttää jatkuvaa työtä perusasioiden kuntoon laittamisessa. Tämä taas vaatii niin johdon, henkilöstön kuin kyberturvallisuuden asiantuntijoiden tietoisuuden lisäämistä kyberturvallisuudesta. Käytännössä tietoisuutta voi lisätä henkilöstön kehittämisen avulla (3.6) ja harjoitustoiminnalla.

4.4 Hajonta mahdollistaa yhteistyön

Kartoituksen tuloksissa on useilla toimialoilla samanlaisina toistuvia kehityskohteita. Samojen haasteiden läpi leikatessa, yhteisten kehityskohteiden avulla voidaan tehokkaasti parantaa parhaita käytänteitä. Tämä tukee myös huoltovarmuuden toteutumista, kun yrityskohtaiset erot kyberturvallisuuden toteutumisessa vähenevät toimialojen sisällä ja välillä. Kyberturvallisuudessa esiintyvät poikkeavuudet häiritsevät tällöin vähemmän toimialojen välisissä riippuvuusketjuissa.

Yhteistyön tukemiseksi on hyvä kehittää olemassa olevia yhteistyörakenteita kuten harjoitustoimintaa, josta ovat esimerkkeinä Digipoolin TIETO-harjoitukset ja Kyberturvallisuuskeskuksen kyberturvallisuustiedonvaihtoon räätälöidyt ISAC-toimialaverkostot. Kokonaisuutta täydentämään on hyvä miettiä toimialojen välille myös uusia yhteistyötapoja, jotka mahdollistavat esimerkiksi toimialojen välisen tilannekuvatiedon vaihtamisen (3.4).

4.5 Reaktiivisessa toiminnassa parhaat kypsyystasot

Kyberturvallisuuteen liittyvistä toimenpiteistä reaktiivinen ja havainnoiva toiminta oli kokonaisuudessa parhaiten toteutettu. Tämä näkyy tuloksissa onnistumisena niin tapahtumien ja poikkeamien hallinnan dokumentoinnissa kuin perustoiminnan jatkuvuuden suunnittelussa: kriittisten palveluiden suojaaminen, suojattavien kohteiden, muutosten ja konfiguraation hallinta on tulosten perusteella kohtuullisesti huomioitu useissa yrityksissä.

Useat tiedossa olevat kyberpoikkeamat ovat saaneet alkunsa identiteettien, käyttövaltuuksien ja pääsynhallinnan ongelmista. Ilmeisesti ongelmakohta on myös toivotusti saanut huomiota tietoturvaloukkausten seurauksena, sillä aihealue ei löydy ensisijaisten kehityskohteiden joukosta. Osa-alueen jatkuva kehitys on jatkossakin välttämätöntä, mutta tulos kertoo, että ratkaisuja on osattu ottaa myös käyttöön. Vastaavasti valmiita malleja ja ratkaisuja on tarjolla yrityksille, joilla on osa-alueessa kehitettävää.

Poikkeamien hallinnan oppaita on vuosien aikana laadittu useiden tahojen toimesta. Myös aiemmissa kehitysohjelmissa toteutettu HAVARO-järjestelmä, ISAC-toiminnan tiedonvaihto ja harjoitustoiminta sekä itse harjoitukset ovat oletettavasti osaltaan edesauttaneet reaktiivisen toiminnan kehittymistä vuosien aikana. Tuloksissa on kuitenkin vaihtelua ja kyberympäristö muuntuu jatkuvasti, joten kehitystyötä on syytä jatkaa ja pitää ajantasaisena.

4.6 Elinkeinoelämä tunnistaa kyberturvallisuuden hankintaketjussa sopimusperusteisesti

Kartoituksessa tuli ilmi, että yritykset osaavat hyvin huomioida jatkuvuuden hallinnan sopimuksissa, kun ne hankkivat osaamista, tuotetta tai palvelua riippuvuusketjussa toisen toimialan yrityksiltä. Sopimuksiin kirjataan, miten palvelun tulee jatkuvuudeltaan toteutua ja mitä seuraa, jos toiminnan katkeaminen tai häiriöt vaikuttavat asiakkaan toimintaan. Tulos antaa hyvät lähtökohdat riippuvuusketjuissa ilmenevien vaikutusten vähentämiselle jatkossakin.

4.7 Sääntely vaikuttaa myönteisesti turvallisuuden edistämiseen

Toimialoja voidaan ohjata turvalliseen suuntaan lakiperusteisesti säädöksillä ja määräyksillä. Ne edistävät myös riippuvuusverkoston turvallisuutta, kun yrityksellä on saatavilla puolueeton tieto, mitä omassa riippuvuusketjussa olevilta eri toimialojen yrityksiltä edellytetään ja mistä ei tarvitse oman turvallisuuden vuoksi erikseen sopia.

Tuloksista havaitaan, että pitkään säännellyt, viranomaisten ohjaamat ja valvomat toimialat asettuvat vertailussa kärkeen. Selvityksessä ei erikseen arvioitu, mikä osuus sääntelyllä on ollut asiaan,

mutta positiivinen vaikutus on havaittavissa niin tilastollisesti kuin työpajakeskustelujen perusteella toimialoja verratessa.

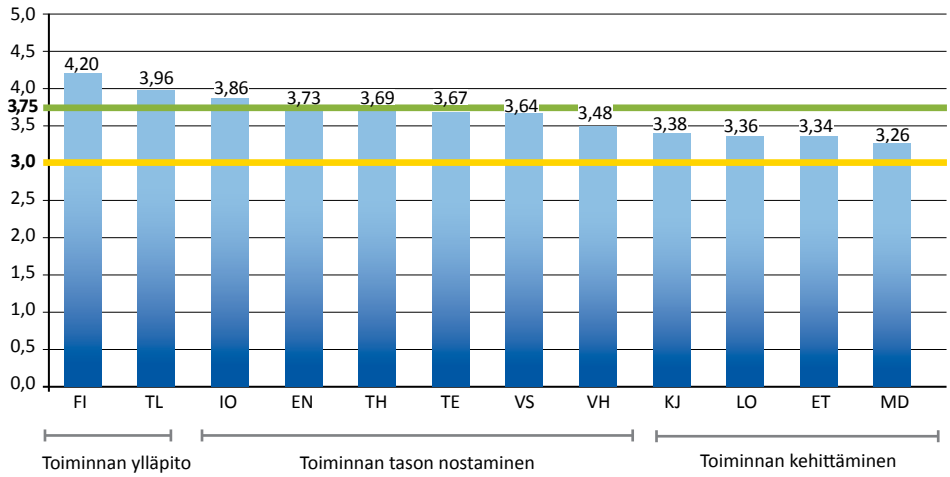
On huomioitava, että sääntely on hidas keino parantaa nopeasti muuntuvaa kyberturvallisuutta. Vaatimuksien kohdentaminen tarkasti on haasteellista uhkien muuntuessa nopeasti. Kokemus myös kertoo, että tasapuolisen sääntelyn laatiminen eri kokoisille organisaatioille ei ole yksiselitteistä. Usein lopputulos kankeuttaa nimenomaan Suomessa yleisten pienten ja keskisuurten organisaatioiden toimintaa. Parhaiten sääntely toimii, kun sen kautta asetetaan vaatimuksille minimitaso. Osaa toimenpiteistä voidaan ohjata varsinkin aluksi kevyempien suositusten avulla. Kriittisimmille toimialoille merkittävässä ohjaavassa asemassa on EU:n verkko- ja tietoturvadirektiivi (NIS-direktiivi), joka on otettu käyttöön 2018, ja jonka kehitys jatkuu.

Lopulta on huomioitava, että yksittäisen yrityksen kyberturvallisuuden tilanne on ensisijaisesti riippuvainen johdon sitoutumisesta ja ohjauksesta – miten vahvasti edellytetyt toimenpiteet on toteutettu ja kannustetaanko niihin oman toiminnan tukemiseksi vai vaatimuksen vuoksi. Parhaimmillaan nämä kohtaavat niin, että regulaatio tukee kyberturvallisuuden toteuttamista.

5 TOIMIALAKOHTAISTEN TULOSTEN PÄÄHAVAINNOT

Kaikilla yhteiskunnalle kriittisillä toimialoilla kyberturvallisuuden taso on vähintään keskinkertainen, eli toimet on määritelty tai suunniteltu. Tämä on hyvä lähtökohta edelleen kohentaa ja yhdenmukaistaa kyberturvallisuutta. On kuitenkin syytä huomioida, että toimialojen välillä sekä niiden sisällä on merkittäviä eroja. Syitä vaihtelevuudelle muodostavat:

- toimijoiden kokoerot
- käytettävissä olevat resurssit
- toimialalla vaikuttava kotimainen ja kansainvälinen regulaatio
- sopimusten myötä tulevat asiakasvaatimukset
- eri toimialat ovat digitalisaation kehityksessä eri vaiheessa.



FI= finanssiala, TL= teleliikenneala, IO= ICT- ja ohjelmistoala, EN= energia-ala, TH= terveydenhuoltoala, TE= teollisuusala, VS= satama- ja merenkulkualat, VH= vesihuoltoala, KJ= kaupan- ja jakelun ala, LO= logistiikka-ala, ET= elintarvikeala, MD= media-ala

Kuva 6. Toimialojen kypsyystaso voidaan jakaa toiminnan ylläpitoon, tason nostamiseen ja kehittämiseen.

Finanssiala ja teleliikenneala ovat saavuttaneet tavoitetason neljä, eli kyberturvallisuus on johdonmukaisesti toteutettu. On tärkeää, että kehitystoimenpiteillä pyritään jatkossa ylläpitämään muuttuvassa ympäristössä saavutettu taso.

Tuloksissa seuraavilla toimialoilla (eli ICT- ja ohjelmistot, energia, terveydenhuolto, vesiliikenne ja satamat, vesihuolto) kyberturvallisuustoimet on varsin laajasti toteutettu suunnitellusti, vaikkakin hajanaisesti osassa toiminnoista ja useissa yrityksissä on vielä kehittämiseen varaa. Tilanteessa on hyvät edellytykset kehittää toimintaa kypsälle, eli johdonmukaisesti toteutetulle tasolle. Toimialojen pääkehitystavoite on tilanteen yhtenäistäminen, mikä johdattelee toiminnan kypsemmälle tasolle.

Digitalisaatiossa suuren murroksen aloittaneet media, logistiikka, elintarvikeala ja kaupan ja jakelun ala ovat tuloksissa saavuttaneet keskinkertaisen tason. Nostaakseen toimialoina kyberturvallisuuden tasoa alojen yritykset tarvitsevat yhtenäisiä tavoitteita ja yhdenmukaista kehitystä, jotta digitalisaation kehityksessä myös kyberturvallisuus tulee samanaikaisesti huomioiduksi.

Kyberturvallisuuden keskinäisriippuvuuksien kannalta on huomionarvoista, että tuloksissa kärkinelikon (finanssi, ohjelmisto ja ict, teleliikenne ja energia) muodostaa sama nelikko kuin perusinfrastruktuurin ytimen (4.1). Kokonaisuuden kannalta on tarkoituksenmukaista, että kyberturvallisuus on edistyksellisimmin hoidettu keskinäisriippuvuuksien perusteella merkittävimmillä aloilla.

Kyberturvallisuusuhkat ovat samankaltaisia kaikilla digitalisoituneen yhteiskunnan toimijoilla, joten uhkien tunnistamista ja hallintaa kannattaa toteuttaa julkisen sektorin ja yksityisen sektorin toimijoiden yhteistyönä. Kyberturvallisuutta tulee kehittää kaikilla tasoilla: yhteiskunnalle elintärkeitä palveluita tuottavissa organisaatioissa, huoltovarmuusorganisaation toimialapooleissa ja koko huoltovarmuusorganisaatiossa. Toimialakohtaisten tulosten tiivistelmät on esitetty liitteissä 1-12.

6 SELVITYKSEN TOTEUTUS

Selvitys toteutettiin valitsemalla kypsyysarviointimalli ja selvitykseen osallistuvat huoltovarmuuskriittiset toimialat ja yritykset. Pisteytys ja tarkentavat selitteet käytiin läpi haastatteluin talvella 2019-2020. Yrityksistä haastatteluihin osallistui liiketoiminnan, tietohallinnon ja turvallisuuden edustajia. Osallistujat tutustuivat ennen haastattelua omatoimisesti kypsyysarvion kysymyksiin, jotta heillä oli ennalta käsitys käsiteltävistä osa-alueista. Kypsyysarvoja suhteutettiin objektiivisen kriteeristön mukaisesti tarkentavien perustelujen avulla. Tämän jälkeen yrityskohtaiset tulokset on yhdistetty toimialakohtaisiksi tuloksiksi. Näin tuloksien vertailukelpoisuutta ja laatua voidaan pitää hyvänä, sillä eri yritysten tulokset on objektiivisesti skaalattu samalle asteikoille.

Osallistujien valinta

Selvitykseen valittiin toimialapoolien avustuksella erikokoisia yrityksiä 12 toimialalta ympäri Suomea, jotta saadaan kattava ymmärrys. Valintaperusteena oli NIS-direktiivi, pooliorganisaatio ja huoltovarmuuspäätös. Toimialojen nimeämisessä jouduttiin tekemään kompromisseja, jotta selvitystyö olisi hallittavissa kuitenkin riittävän laajalla otoksella erilaisia organisaatioita. Kansallisen kokonaiskuvan lisäksi nähtiin tärkeänä tuottaa toimialakohtaisia tuloksia.

Toimialojen organisaatioihin sisältyi seuraavia tuotanto- tai palvelualan tahoja:

1. **Elintarvike:** alkutuotanto ja elintarviketeollisuus
2. **Energia:** sähköntuotanto ja -jakelu sekä öljynjalostus
3. **Finanssi:** pankki, vakuutus
4. **ICT ja ohjelmisto:** tietoturva, ohjelmistotuotanto
5. **Kauppa ja jakelu:** vähittäiskauppa, tukku, jakelu
6. **Logistiikka:** logistiikka- ja kuljetuskeskukset
7. **Media:** graafinen, joukkoviestintä
8. **Teleliikenne:** operaattorit, verkkourakointi
9. **Teollisuus:** kemia ja rakennus
10. **Terveydenhuolto:** lääketuotanto, logistiikka, sekä hoito
11. **Vesihuolto:** vedentuotanto, -jakelu ja -puhdistus
12. **Vesiliikenne ja satamat:** satamalaitos ja -operaattori

Yhteensä mukana oli yli 100 yritystä. Toimialoittain edustettuna yrityksiä oli vähintään kuusi, jotta alalta oli mukana erilaisia toimijoita ja yksittäisen yrityksen toiminnan merkitys ei vaikuta merkittävästi koko toimialan tuloksiin. Yritykset valittiin kunkin toimialan organisaatioista liikevaihdon, maantieteellisen sijainnin, huoltovarmuusmerkittävyyden ja vapaaehtoisuuden perusteella.

Käytetty kyberturvallisuuden kypsyysarviointimalli

Selvityksessä käytetty kyberturvallisuuden kypsyysarviointi perustuu Kyberturvallisuuskeskuksen kybermittari-työkalun pohjaksi suomentamaan ja laajentamaan Yhdysvaltain energiaviraston C2M2 (Cybersecurity Capability Maturity Model) arviointimalliin. Laajennuksessa on huomioitu NIST:n Cyber Security Framwork -mallin kriittisen infrastruktuurin arviointiosuudet Saksassa ja Australiassa. Kokonaisarviointi sisältää noin 300 kysymystä hyvin yksityiskohtaisiin toteutuksiin saakka. Selvityksessä haluttiin kiinnittää huomiota nimenomaisesti liiketoimintariskinäkökulmaan, joten mukaan poimittiin sitä kuvaavat C2M2:n kaksi ylintä tasoa (11 aluetta ja 30 tavoitetta). Lisäksi arviointimallia muokattiin käyttämällä prosessikypsyysarvioinnin standardin (CMMI) kypsyystasoja C2M2:n tehtävä- ja tavoitetasojen minimisuoritusvaatimuksien sijaan alla olevan arviointiasteikon mukaisesti.

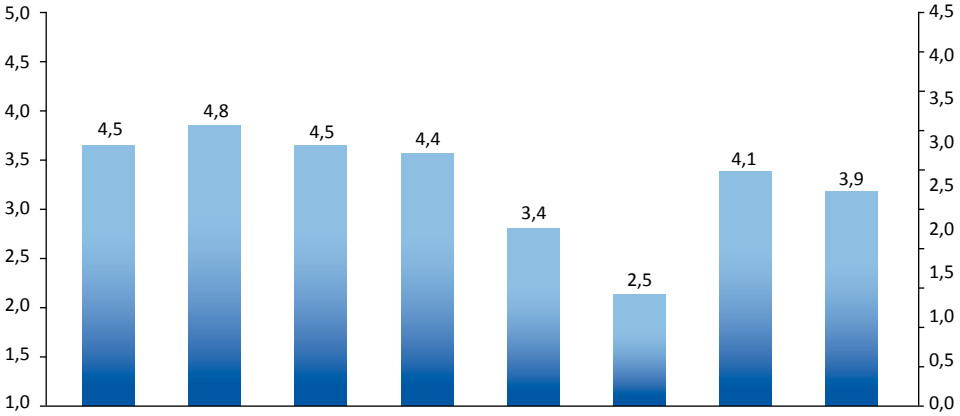
Taso	Selite
5	Kehitetään jatkuvasti riskilähtöisesti
4	Tehdään johdonmukaisesti
3	On määritelty tai suunniteltu
2	Tehdään vaihtelevasti ja/tai osittain
1	Ei tehdä

Mallin liiketoimintariskilähtöiset kysymykset kattavat seuraavat osa-alueet:

1. Kriittisten palvelujen suojaaminen
2. Riskienhallinta
3. Suojattavien kohteiden, muutosten ja konfiguraation hallinta
4. Kyberturvallisuuden hallintajärjestelmä
5. Toimitusketjujen ja ulkoisten riippuvuuksien hallinta
6. Identiteetin-, pääsy- ja käyttöoikeushallinta
7. Tapahtuminen ja poikkeamien hallinta, toiminnan jatkuvuus
8. Tiedonjako ja viestintä
9. Tilannekuva
10. Uhkien ja haavoittuvuuksien hallinta
11. Henkilöstöhallinta

Tulosten esittäminen

Tuloksista on valmistunut yrityskohtaiset raportit, jonka jokainen yritys on saanut haastattelutilaisuuden päätteeksi. Tämän jälkeen toimialakohtaiset tulokset on yhdistetty toimialaa koskeviksi päähavainnoiksi kysymyskohtaisesti ja ne on arvioitu niin liiketoimintariskilähtöisesti, riippuvuuslähtöisesti kuin riskiperusteisesti. Eri arviointitavat antavat hieman erilaiset tulokset, joita voidaan hyödyntää eri kehitystarpeissa. Toimialojen tuloksista on lisäksi laadittu koonti, joka on toimitettu osallistuneiden yritysten lisäksi kehitystyöhön osallistuville tahoille. Näiden perusteella on poikkileikkaavista ja eri arviointitavoilla toistuvista kehityskohteista koottu nyt käsissä oleva tiivistelmä.



Kuva 7. ***Esimerkki yhden toimialan tuloksista erään kysymyksen kohdalla. Jokainen pylväs kuvastaa eri yrityksen tulosta.***

7 LIITTEET

Liite 1

ELINTARVIKETEOLLISUUS

KYPSYYSTASO
3,34

JOHDONMUKAISUUS
36,3%

ERITYISPIIRRE

Alaa leimaa toiminnan vahva laatuohjaus.

ONNISTUMINEN

- Tiukat laatukriteerit
- Panostus tuoteturvallisuuteen
- Häiriötilanteiden hallinta
- Tuotantoketjun riippuvuuksien analysointi

KEHITYSKOHTEET

- Turvallinen ohjelmistokehitys
- Kyberturvallisuusarkkitehtuuri
- Kyberturvallisuuteen liityvän tiedon jakaminen

Liite 2

ENERGIA

KYPSYYSTASO
3,73

JOHDONMUKAISUUS
49,7%

ERITYISPIIRTEET

Kaikki toimialat ovat vahvasti riippuvaisia energiasta. Fossiilisista energialähteistä luopuminen on murros, joka mullistaa myös huoltovarmuuden.

ONNISTUMINEN

- Tunnistaneet ja suojanneet kriittiset palvelunsa
- Operatiivinen toiminta poikkeamien ja jatkuvuuden hallinnassa on hyvällä tasolla

KEHITYSKOHTEET

- Turvallinen ohjelmistokehitys
- Yhteinen operatiivinen tilannekuva
- Kyberturvallisuusarkkitehtuuri

Liite 3

FINANSSI

KYPSYYSTASO
4,20

JOHDONMUKAISUUS
80,8%

ERITYISPIIRTEET

Vahvasti reguloitu ala, jossa huomioitu operatiivisen toiminnan valvonta. Digitaalinen, nopeasti kehittyvä toimintaympäristö asettaa vaatimuksia infrastruktuurille ja sen turvallisuudelle.

ONNISTUMINEN

- Hyvin varmistettu ja resursoitu perustietoturva
- Johdon tuki tietoturvallisuuden ylläpidolle ja kehittämiselle

KEHITYSKOHTEET

- Jatkuvuuden suunnittelu
- Kyberturvallisuusriskien hallinta
- Haavoittuvuuksien hallinta

Liite 4

ICT- JA OHJELMISTOALA

KYPSYYSTASO
3,86

JOHDONMUKAISUUS
59%

ERITYISPIIRTEET

Keskeinen rooli kyberturvallisuudessa, sillä toimialan suunnittelemia, toteuttamia ja ylläpitämiä palveluita ja ratkaisuja käytetään myös kaikilla muilla toimialoilla.

ONNISTUMINEN

- Kyberturvallisuustapahtumien eskalointi ja häiriöiden julistaminen
- Kyberturvallisuustapahtumien ja häiriöiden käsittely

KEHITYSKOHTEET

- Yhteinen operatiivinen tilannekuva
- Kyberturvallisuusarkkitehtuuri
- Riippuvuusriskien hallinta

Liite 5

KAUPPA- JA JAKELU

KYPSYYSTASO
3,38

JOHDONMUKAISUUS
34,2%

ERITYISPIIRRE

Materiaalivirtoja ohjataan, seurataan ja raportoidaan täysin automatisoidusti.

ONNISTUMINEN

- Korkea toimitusketjujen tuntemus
- Kyberturvallisuuden huomiointi ulkoisten riippuvuuksien hallinnassa

KEHITYSKOHTEET

- Kyberturvallisuuteen liityvän tiedon jakaminen
- Seuranta
- Haavoittuvuuksien hallinta

Liite 6

LOGISTIIKKA

KYPSYYSTASO
3,36

JOHDONMUKAISUUS
39,1%

ERITYISPIIRRE

Logistiikkakeskukset ovat hyvin pitkälle automatisoituja ja varastorobotiikan kyberhäiriötilanteessa manuaalista korvausmenetelmää ei ole.

ONNISTUMINEN

- Hallintajärjestelmä
- Kyberturvallisuusstrategia
- Riskinhallintastrategia
- Kyberturvallisuusarkkitehtuuri
- Johdon tuki

KEHITYSKOHTEET

- Kyberturvallisuuteen liityvän tiedon jakaminen
- Kriittisten palvelujen ja niiden riippuvuuksien tunnistaminen
- Kyberturvallisuushenkilöstön kehittäminen

Liite 7

MEDIA

KYPSYYSTASO
3,26

ERITYISPIIRTEET

Merkittävät kuormituspiikit palvelualustoilla. Digitalisaatio edennyt pitkälle ja pilvipalvelut vahvasti käytössä. Erityiset tietoturva-haasteet liittyen lähdesuojaan.

JOHDONMUKAISUUS
19,5%

ONNISTUMINEN

- Media-alalla on ansiokkaasti todettu, että digitaalisessa virrassa voi levitä haitallisia uutisia

KEHITYSKOHTEET

- Seuranta
- Uhkien tunnistaminen ja hallinta
- Yhteinen operatiivinen tilanne-kuva

Liite 8

SATAMAT JA MERENKULKU

KYPSYYSTASO
3,64

ERITYISPIIRRE

Toiminta jakaantuu lukuisille pienille toimijoille.

JOHDONMUKAISUUS
51,3%

ONNISTUMINEN

Kyberturvallisuuden määrittelyt

- pääsääntöisesti tehty
- otettu käyttöön lähes koko-naisvaltaisesti

KEHITYSKOHTEET

- Kyberturvallisuustietoisuuden lisääminen
- Kyberturvallisuuden vastuut
- Riippuvuusriskien hallinta

Liite 9

TELELIIKENNE

KYPSYYSTASO
3,96

JOHDONMUKAISUUS
65%

ERITYISPIIRRE
Kaikki toimialat ovat riippuvaisia teleliikenteestä ja sen toimivuudesta.

ONNISTUMINEN
- Poikkeamien havaitsemisen automatisointi
- Häiriöiden hallinta

KEHITYSKOHTEET
- Kyberturvallisuusarkkitehtuuri
- Yhteinen operatiivinen tilannekuva
- Turvallinen ohjelmistokehitys

Liite 10

TEOLLISUUS

KYPSYYSTASO
3,67

JOHDONMUKAISUUS
52,7%

ERITYISPIIRRE
Alan toimijoiden hajanaisuuden vuoksi sääntely ja ohjaus alalla hyvin vähäistä.

ONNISTUMINEN
- Riippuvuuksien tunnistaminen
- Pääsyoikeuksien hallitseminen
- Työsuhteen elinkaaren hallinta
- Toimiala tasaisen hyvä eri tavoitteiden osalta

KEHITYSKOHTEET
- Yhteinen operatiivinen tilannekuva
- Kriittisten palvelujen hallinta
- Kyberturvallisuuteen liittyvän tiedon jakaminen

Liite 11

TERVEYDENHUOLTO

KYPSYYSTASO
3,69

ERITYISPIIRRE
Hyvin erilaisia
toimintaympäristöjä hallittavaksi
- toimistoverkko
- lääkinnälliset laitteet
- potilastiedot

Tietoturvan lisäksi tietosuojan hallinta.

JOHDONMUKAISUUS
48,5%

ONNISTUMINEN
- Riippuvuuksien tunnistaminen toimitus- ja kumppanuusketjuissa

KEHITYSKOHTEET
- Kyberturvallisuushenkilöstön kehittäminen
- Yhteinen operatiivinen tilannekuva
- Seuranta

Liite 12

VESIHUOLTO

KYPSYYSTASO
3,48

ERITYISPIIRRE
Tele- ja IT-infra usein kaupungin
tai kunnan ylläpidossa.

JOHDONMUKAISUUS
41,7%

ONNISTUMINEN
- Varautuminen hyvin suunniteltu ja toiminnot voidaan yleisesti hoitaa manuaalisesti ("pimeäajona")

KEHITYSKOHTEET
- Seuranta
- Kyberturvallisuusriskien seuranta
- Lokituksen toteutus

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY