Yhteenveto Digiturvakompassi-podcasteista

24.8.2021

Sisällys

1. TIIVISTELMÄ

Raportti on laadittu Digiturvakompassin haastattelumuotoisten podcast-jaksojen numero 1-21 sisällöistä. Se sisältää tiivistelmiä podcastien digitaalista turvallisuutta käsittelevistä teemoista ja niihin liittyvistä podcasteissa esiin nousseista podcast-vieraiden kertomista näkökulmista. Raporttiin on poimittu podcast-jaksoista kysymyksittäin keskeisimmät läpikäydyt asiat ja laadittu yhteenveto keskustelujen keskeisestä annista. Ensimmäisen ja viimeisen kysymyksen osalta yhteenveto on tekstimuodossa ja muista kysymyksistä yhteenveto on laadittu taulukkomuodossa jatkokäyttöä varten.

Yhteensä podcasteissa on vieraillut 21 henkilöä, joista 12 oli ministeriöistä. He edustivat yhdeksää eri ministeriötä. Virastoista, keskuksista ja Turvallisuuskomiteasta oli neljä podcast-vierasta ja kunnista kaksi kaupunginjohtajaa sekä Kuntaliiton edustaja. Lisäksi podcast-vieraana oli valtion kyberturvallisuusjohtaja ja Aalto-yliopiston kyberturvallisuuden työelämäprofessori.

Digiturvakompassin jaksoissa on käytetty pääosin seuraavaa kysymysrunkoa:

1 Miten ministeriö liittyy digiturvallisuuteen?
2 Covid ja pandemia – vaikutukset?
3 Mitä on luottamus?
4 Mitkä ovat podcast-vieraan vinkit henkilökohtaisessa elämässä digiturvan toteuttamiseksi?

Ensimmäisen kysymyksen osalta podcast-vieraat kertoivat näkemyksiään ja omia painotuksiaan siitä, miten heidän edustamansa organisaatio liittyy digiturvallisuuteen ja miten heillä edistetään digitaalista turvallisuutta sisäisesti ja yhteiskunnassa. Ensimmäisellä kysymyksellä pyrittiin avaamaan kuulijoille eri toimijoiden roolia ja tehtäviä yhteiskunnan digitaalisen turvallisuuden varmistamisessa. Podcast-vieraiden näkemykset kertovat heidän painotuksistaan tehtävien osalta. Keskustelun perusteella voidaan myös esimerkiksi arvioida mahdollisia yhtäläisyyksiä ja yhteistyötä digitaalisen turvallisuuden tehtävissä. Keskustelut voidaan jaotella podcast-vieraiden perusteella ministeriöihin, virastoihin ja laitoksiin, kuntatoimijoihin sekä yksittäisiin henkilöihin ja yhteistyötoimijoihin.

Covid 19 -pandemia pandemian osalta tarkasteltiin sen vaikutuksia digitaalisen turvallisuuden jatkokehittämiseen ja mahdollisiin onnistumisiin sekä kehityskohteisiin. Podcasteissa ajankohtaissisältönä nousivat esiin pandemian lisäksi ajankohtaisena asiana Koronavilkun käyttöönotto. Organisaatioiden pakotettu sisäinen ja ulkoinen digiloikka toi paljon kehitystä, mutta samalla se on kasvattanut digitaalisen turvallisuuden uhkia. Korona-aikana viranomaisviestintää on erityisesti hankaloittanut kriisitilanteessa puhjennut informaatiopandemia, joka on vaikeuttanut tilannekuvan luomista. Lisäksi COvid19 -pandemia edellytti laajaa viranomaisyhteistyötä eri toimialoilla eri toimivaltaisten viranomaisten piirissä sekä haastoi sisäisesti viranomaisten toiminnan johtamista ja keskitettyä viestintää. Tieto- ja viestintäverkot kestivät Suomessa melko hyvin siirtymän etätöihin ja digipalveluihin, mutta mahdolliset digiturvaprosesseissa tehdyt poikkeukset, jotka mahdollistivat siirtymän poikkeustilan-

teeseen, tulee tarkastella kriittisesti ja mahdolliset turvallisuusaukot tulle korjata. Pandemiaa seuranneessa kriisissä oli erityisesti hyötyä aiemmista harjoituksista ja varautumissuunnittelusta, jolloin poikkeusoloissa pystyttiin keskittymään muihin esille tuleviin asioihin. Pandemian seurauksena myös moni yksittäinen ihminen otti henkilökohtaisen digiloikan ja digitaalinen palveluvalikoima monipuolistui, mutta se on koetellut vahvasti henkilökohtaisen elämän näkökulmasta monien kriisinsietokykyä.

Podcastissa kysyttiin vierailta heidän näkemyksestään luottamuksesta ja kuinka sitä voitaisiin ylläpitää ja kehittää digitaalisen turvallisuuden osalta. Keskeiseksi nousi instituutioihin ja organisaatioihin kohdistettu yhteiskunnallinen luottamus, jota viranomaisten tulee rakentaa ja vaalia. Luottamus on erityisen tärkeää turvallisuussektorilla ja kriittisissä palveluissa, jossa se on perusta kaikelle toiminnalle ja jossa sitä ei voi menettää kertaakaan. Tietojärjestelmien ja tiedon suojaamiseen osalta luottamuksen eteen tulee tehdä jatkuvasti työtä ja käytännön toimenpiteitä, jotta palvelun vaikuttavuus ja laatu ei heikkene. Ihmisten välisenä luottamus näyttäytyy tunteena ja kokemuksena, joka kannustaa yhdessä tekemiseen. Tämän vuoksi myös verkostoissa on tärkeää olla vahva sisäinen luottamus yhteistyön mahdollistamiseksi. Luottamuksen ylläpito perustuu avoimuuteen, rehellisyyteen ja läpinäkyvyyteen, minkä lisäksi sitä tulee ylläpitää myös oikeusvaltioperiaatteen, hyvän hallintotavan ja lainsäädäntöprosessin kattavuuden kautta. Yrityksien osalta avoimuuden puute voi heikentää luottamusta sen toimintaan. Luottamuksen voi menettää hyvin helposti, joten luottamus esimerkiksi hybridiuhkien osaamiskeskuksen perustamisen osalta on Suomelle kilpailuetu. Lisäksi on huomioitavaa, että luottamusta voidaan käyttää myös väärin huijaustarkoituksessa.

Podcast-vierailla oli myös omia vinkkejä koskien digitaalista turvallisuutta. Podcast-vieraat painottivat vinkkeinä erityisesti oikeanlaista asennoitumista toimintaan digimaailmassa ja siellä kohdattaviin haasteisiin sekä ymmärryksen lisäämiseen operatiivisella tasolla. Yksityiskohtaisemmin podcast-vieraat painottivat digiturvavinkeissä päätelaitteisiin ja sovelluksiin, tietoliikenneverkkoihin, fyysiseen ja sosiaaliseen ympäristöön, salasanoihin, tunnistautumiseen, tiedonhallintaan, asumiseen ja kodin laitteisiin liittyviä digiturvallisuusvinkkejä.

2. YKSITYISKOHTAINEN YHTEENVETO KESKUSTELUISTA

2.1. MINISTERIÖIDEN JA MUIDEN TOIMIJOIDEN TEHTÄVÄT YHTEISKUNNAN DIGITURVALLISUUDESSA

Ensimmäisellä kysymyksellä pyrittiin avaamaan kuulijoille eri toimijoiden roolia ja tehtäviä yhteiskunnan digitaalisen turvallisuuden varmistamisessa. Keskustelut voidaan jaotella podcast-vieraiden perusteella ministeriöihin, virastoihin ja laitoksiin, kuntatoimijoihin sekä yksittäisiin henkilöihin ja yhteistyötoimijoihin.

Ministeriöistä valtioneuvoston kanslia koordinoi valtioneuvoston yhteisen hallinnon laajaa kokonaisuutta. Ministeriö vastaa osittain digitaalisen turvallisuuden toimintapolitiikasta ja operatiivisesta turvallisuudesta valtioneuvoston kokonaistasolla. Politiikan lisäksi ministeriössä työskennellään myös käytännön toimintaprosessien ja niitä tukevien tietojärjestelmien parissa, joissa korostuu syvä tietämys ja riskienhallinta.

Ulkoministeriö on podcastin mukaisesti Suomen ja suomalaisten etujen ajaja maailmalla. Ministeriö edistää Suomen ja suomalaisten turvallisuutta ja hyvinvointia sekä toimii turvallisen ja oikeudenmukaisen maailman hyväksi. Maailman muutos aiheuttaa haasteita pienen ulkomaankaupasta riippuvaisen maan kannalta.

Sisäministeriö tukee hallinnonalaa digitalisaatioon liittyvissä mahdollisuuksissa laatimalla tiekarttaa sisäisen turvallisuuden digitalisaation kehittämiseen ja laajaa turvallisuuden hallintamallia. Turvallisuusviranomaisten toiminnassa digiturvallisuus on osa jatkuvan valmiuden periaatetta ja kokonaisturvallisuuden mallia, jossa huolehditaan toimivasta viestinnästä, keskinäisestä yhteistyöstä ja kansalaisille tarjottavista sähköisistä turvallisuus- tai lupapalveluista. Palveluiden saatavuutta tehostetaan hyödyntämällä uusia toimintatapoja. Toteutuksien tulee noudattaa yhteistä turvallisuus- ja kokonaisarkkitehtuuria ja tukeutua julkisen hallinnon tietovarantoihin ja muihin digitaalisia palveluihin. Kuitenkin hyödynnettäessä avointa tietoa ja rakennettaessa uusia toimintamalleja podcastien mukaan tulee aina huolehtia, että turvallisuusviranomaisilla on mahdollisuus hallita kokonaisuutta niin toimintavarmuuden, luotettavuuden kuin turvallisuudenkin näkökulmasta. Digitaalinen turvallisuus on myös osa kansallisen turvallisuuden takaamista siviili- ja sotilastiedustelulakien ja yksityiselämän suojan suhteen tarkoituksena suojata kansallinen suvereniteetti erilaisia uhkia vastaan.

Puolustusministeriön hallinnonalan toimintoihin liittyy paljon tietotekniikkaa, sovelluksia ja ohjelmistoja, joissa käsitellään suojattavaa sensitiivistä tietoa. Siksi digiturvaan suhtaudutaan vakavasti esimerkiksi rakentamalla sisäistä ISO27001-standardin mukaista hallintajärjestelmää ja osallistumalla valtioneuvoston yhteisten tietojärjestelmien vaatimusmäärittelyn, eri ministeriöiden kehitystyöhön ja lainsäädäntöhankkeisiin puolustussektorin näkökulmasta. Hallinnonalalla ohjataan digitur-

vallisuuden ja kyberpuolustuksen kehittämistä, sekä varmistetaan puolustusvoimien etu lainsäädännön tasolla. Hallinnonalan osalta ministeriössä ohjataan myös organisaatioturvallisuutta, teknistä turvallisuutta, kansallisen määrätyn turvallisuusviranomaisen tehtävää ja avaruustoiminnan valvontaa.

Valtioneuvostoa avustava Turvallisuuskomitea on podcast-vieraan mukaan varautumisen strategisen tason yhteistyöelin. Kokonaisturvallisuusmallin mukaisesti se pyrkii yhteensovittamaan ja koordinoimaan yhteiskunnan varautumista viranomaisten lisäksi myös elinkeinoelämän osalta toimien kansainvälisessä yhteistyössä, ja seuraten turvallisuuden isoa kuvaa. Komitea on vastannut yhteiskunnan turvallisuusstrategian ja kyberturvallisuusstrategian laadinta- ja päivitystyöstä.

Valtiovarainministeriö vastaa podcast-vieraan mukaan julkisen hallinnon kokonaisuuden koordinaatiosta ja sillä on koordinaatiovastuu myös ICT-turvallisuudesta. Talouden näkökulmasta ministeriö pyrkii edistämään digitalisaatiota ja toimintaa teknologian avulla ja saamaan sen avulla tuottavuutta aikaiseksi, kuten lisäämällä sähköistä asiointia ja etäasiointia. Työnteon osalta digitalisaatio ja lisääntyneet etätyöt ovat vähentäneet matkustamista ja pidemmällä aikavälillä myös toimipaikkakustannukset voivat laskea.

Hallinnonalalla toimivan Digi- ja väestötietoviraston johtolauseena on edistää yhteiskunnan digitalisaatiota. Käytännössä podcast-vieraan mukaan virastossa pyritään auttamaan virastoja, kuntia ja muita toimijoita yhteentoimivien palveluiden rakentamisessa digitaalisin keinoin. Tällaisissa palveluissa voidaan mahdollistaa paremmin tiedonsiirrot ja yhteiset pelisäännöt palveluiden välillä. Yksi tehtävistä on tietoturvaan liittyvä neuvonta ja operatiivisen Vahti-toiminnan koordinointi.

Liikenne- ja viestintäministeriö vastaa podcast-vieraan mukaan viestintäverkkojen ja viestintäpalvelujen tietoturvallisuuteen liittyvästä lainsäädännöstä, strategiatyöstä ja yleisestä ohjauksesta. Viestintäverkot ja -palvelut ovat ikäänkuin digitaalisen yhteiskunnan selkäranka, sillä kaikki yhteiskunnan digitaaliset palvelut toimivat niiden päällä. Hallinnonalalla toimivan Traficomin Kyberturvallisuuskeskus valvoo sähköisen viestinnän palveluista annetun lain velvoitteita, jota on laajennettu viime vuosina koskemaan kaikkea tietoturvatoimintaa.

Liikenne- ja viestintäministeriöön on sijoitettu myös valtion kyberturvallisuusjohtaja, jonka virka perustuu valtioneuvoston vuonna 2019 hyväksymään kyberturvallisuusstrategiaan. Tehtävänä kyberturvallisuusjohtajalla on laatia kyberturvallisuuden kehittämisohjelma 8-10 vuoden ajalle, minkä tavoitteena on kyvykkyyksien synnyttäminen Suomeen kyberturvan ekosysteemin varmistamiseksi. Kehittämisohjelma on vastaanotettu hyvin ja se tulee podcast-vieraan mukaan todennäköisesti rahoituksen osalta menemään eteenpäin investointina tulevaisuuteen. Elinkeinoelämä on vahvasti mukana yhteisen ekosysteemin rakentamisessa kääntämässä riskejä mahdollisuuksiksi ja tulevaisuusinvestoinneiksi. Lisäksi kyberturvallisuusjohtaja on mukana esimerkiksi Haukka-hankkeen toimeenpano-ohjelmassa ja Huoltovarmuuskeskuksen kriittisen infran kokonaisuudessa.

Sosiaali- ja terveysministeriön hallinnonalalla erityisesti terveydenhuolto on tieto- ja tietojärjestelmäintensiivistä. Asiakas- ja potilastietoihin on kohdistunut jo pidemmän aikaa väärin perusteltua tai rikollista kiinnostusta. Tietoturva on tunnistettu asiakas- ja potilastietojärjestelmissä kriittiseksi, ja

asiakastietolaki asettaa sille keskeiset vaatimukset. Lakimuutokset ovat vireillä viranomaisten roolin selkeyttämiseksi ja valvontatoiminnan vahvistamiseksi, kuin myös rekisterinpitäjien, sote-tuottajien ja Kanta-palveluiden vaatimusten selkeyttämiseksi. Ministeriö osallistuu myös tulevan sosiaali- ja terveysuudistuksen lainsäädännön valmisteluun, missä digitaalinen turvallisuus on myös huomioitava.

Maa- ja metsätalousministeriön monimuotoisella hallinnonalalla digitaalisuuden keskiössä ovat EU:n maataloustukiprosessit ja kiinteistö- sekä peruspaikkatiedot, mutta myös muilla ministeriön alueilla on panostettava vahvemmin digiturvaan. Ministeriö vastaa valtioneuvostotason yhteistyöstä ja ministeriötason varautumisesta. Ministeriöllä on oma tietoturvan hallintamalli ja tietoturvapolitiikka, joiden mukaisesti se toteuttaa esimerkiksi tiedonhallintalain vastuitaan, käsittelee poikkeamia ja raportoi johdolle. Ministeriö vastaa myös yleisesti hallinnonalasta, jota se seuraa tietoriskin osalta ja ylläpitää yleisen tilannekuvaa. Operatiivinen vastuu digiturvasta on hallinnonalan virastoilla.

Työ- ja elinkeinoministeriö luo toimintaedellytyksiä yrityksille ja auttaa kasvua myös digiturvallisuuden alueella. Ministeriön varautumis- ja valmiusasiantuntijat avustavat ja tukevat kansliapäällikköä varautumisen ja turvallisuuden tehtävissä. Ministeriön hallinnonalalla toimii Huoltovarmuuskeskus, jolla on pitkät perinteet digitaalisen turvallisuuden kehittämisessä esimerkiksi haavoittuvuustietojen jakamiseen keskittyvän CERT -toiminnan ja Kyberturvallisuuskeskuksen rahoittajana, sekä yksityisen ja julkisen sektorin datan turvallisen pankkiholvin eli Suomen Huoltovarmuusdatan rakentajana. Huoltovarmuuskeskus on lisäksi Kyberturvallisuus 22 -hankkeessa kehittänyt yhteisiä palveluita pääosin Kyberturvallisuuskeskuksen kanssa, sekä edistänyt toimialojen halukkuutta ja innokkuutta kehittää kyberturvallisuutta. Toimialojen tietoturvan suhteen Huoltovarmuuskeskus on myös fasilitoinut toimialakohtaisia yhteiskunnallisia pooleja, joissa kehitetään esimerkiksi kriittisten toimintojen kyberturvaa, sekä ylläpitänyt Tieto-harjoitusten toimintaa.

Kuntien ja kaupunkien edustajat peräänkuuluttivat kuntien mukana oloa digitaalisen turvallisuuden kehittämisessä ja käyttöönotossa yritysekosysteemin ja tulevan teknologiakehityksen näkökulmista. Jos kunta ei ole sitoutunut digitaaliseen turvallisuuteen, digitaalinen turvallisuus saattaa olla kunnissa päälle liimattua. Kaupunkien ja kuntien digiturvarooli on korostunut esimerkiksi koronavirustilanteeseen liittyvissä toimenpiteissä. Kuntien etujärjestön Kuntaliiton roolina on huolehtia kuntien toimintaedellytyksistä tarjoamalla ja fasilitoimalla kunnille erilaisia asiantuntija- ja tietopalveluita esimerkiksi digiturvaan liittyen sekä ylläpitämällä tietosuoja- ja tietoturvavastaavien verkostoa. Kuntaliitto on toiminut myös yhteistyössä Kyberturvallisuuskeskuksen kanssa väylänä kunnille tavoittaa viranomaisten palvelut.

2.2. COVID 19 -PANDEMIAN VAIKUTUKSET DIGITAALISEEN TURVALLISUUTEEN

Covid 19 -pandemia tuli ajankohtaiseksi julkisen hallinnon digitaaliseen turvallisuuteen vaikuttavaksi tekijäksi ensimmäisten podcast-jaksojen jälkeen, jolloin se otettiin osaksi perushaastattelurunkoa. Pandemian vaikutuksia ei käsitelty jokaisessa podcast-jaksossa. Pandemian vaikutuksia eriteltiin jaksoissa seuraavien kokonaisuuksien mukaisesti.

Vaikutukset digitaalisen turvallisuuden jatkokehittämiseen	Pandemiasta ja sitä seuranneesta kriisistä tulee tehdä realistinen arvio, missä onnistuttiin ja mitä oppeja on hyvä viedä eteenpäin, sekä missä on jatkossa parannettavaa. Onnistumisten osalta tulee vakiinnuttaa hyväksi havaittuja käytäntöjä ja digitaalisia ratkaisuja sekä esimerkiksi kehittää EU:n sähköistä hallintoa. Osa ratkaisuista oli jo olemassa ennen pandemia-aikaa, joten jatkossa on parannettava palveluiden riittävän aikaista käyttöönottoa, esimerkiksi opetuksessa. Pandemia ei ollut yllätys asiantuntijoille, ja jatkossa energian ja työn murrokset aiheuttavat myös muita isompia muutostarpeita. Podcastissa mainittiin LVM:n laaja-alainen Digitaaliset keinot koronaviruskriisin jälkihoidossa -työryhmä.
Organisaatioiden pakotettu sisäinen ja ulkoinen digiloikka	Etätyön ja -palveluiden aiheuttama pakotettu digiloikka oli osittain nopeasti tapahtunut eteenpäin kaatuminen. Tietyissä organisaatioissa ja palveluissa olivat paremmat lähtökohdat ja kyvykkyydet. Mahdollisti kehitystä ja pysyviä ratkaisuja, kuten uudet palvelukanavat ja vahvan tunnistuksen suojausmenetelmät. Kuitenkin hankaloittanut työtehtäviä ja luonut organisaatioille riskitekijöitä. Lisääntynyt tarve digitaalisen toimintaympäristön turvallisuusratkaisuille.
Viranomaisviestintä kriisitilanteessa suhteessa informaatiopandemiaan	Kriisi vaati keskushallinnolta nopeaa reagointia ja tiedotuskykyä. Digitalisaatio mahdollistaa reaaliaikaisen tiedonjaon, mutta myös vaikeuttaa toimivaltaisten viranomaisten viranomaisviestintää. Suuri määrä tietoa eri alustoilla haastaa selkeän viestinnällisen kokonaiskuvan. Tämä suuri määrä muuta kuin viranomaisviestintää vaikeuttaa tilannekuvan luontia ja mahdollistaa valeuutisten, dis- ja misinformaation levittämisen ns. informaatiopandemiana. Dis- ja misinformaation levittämisen ehkäiseminen vaatii sisäistä ja kansainvälistä yhteistyötä. Suomessa tilannetta helpottaa kansalaisten korkea koulutustaso ja medialukutaito.

Tieto- ja viestintäverkot	Pandemiasta johtunut kriisi ei vaikuttanut suuresti suomalaisen tietoyhteiskunnan tietoverkkoihin, sillä perusinfra ja valokuitu mahdollistivat sujuvan siirtymän ja turvallisen sekä vakaan toiminnan. Suomessa ei jouduttu laskemaan palvelun laatua, sillä verkossa liikkuu muutenkin suuret bitti- ja datamäärät. Tämä ei ole itsestäänselvyys esimerkiksi Keski-Euroopassa. Sen johdosta onkin saatu lisäpanostuksia kansainvälisiin turvallisiin kommunikaatioyhteyksiin.
Haasteet ja poikkeukset digiturvaprosesseissa	Kriisin osalta tulee tarkastella, ollaanko nopeassa siirtymässä etäyhteyksien varaan poikettu normaaliolojen digiturvan vaatimuksissa. Poikkeukset eivät saa jäädä pysyviksi, sillä turvallisuusaukot voivat vaikuttaa julkisten palvelujen turvallisuuteen ja luotettavuuteen. Pakollinen digiloikka aiheutti haasteita esimerkiksi turvaluokiteltujen tietojen käsittelylle ja vaatimuksia tartunnanjäljitykseen käytetyille ratkaisuille, joiden tuli täyttää juridiset ja tekniset vaatimukset arkaluonteisen henkilötiedon käsittelystä.
Viranomaisyhteistyö	Viestinnän lisäksi haasteena oli osaltaan se, että kriisi kosketti montaa viranomaista. Positiivinen kokemus viranomaisyhteistyöstä oli Koronavilkun laaja-alainen valmistelutyö, joka tehtiin poikkihallinnollisesti, tehokkaasti ja nopeasti. Sovelluskehityksessä huomioitiin myös tietoturva ja tietosuoja, jolle myös hallinnon ulkopuoliset tietoturva-asiantuntijat antoivat kiitosta, ja kansalaiset myös osoittivat luottavansa sovellukseen sen korkeiden käyttöönottomäärien perusteella.
Muutokset virastojen sisäiseen toimintaan	Kriisi aiheutti sisäisen haasteen viranomaisorganisaatioiden nopealle reagoinnille, tilannekohtaiselle johtamiselle ja toimeenpanolle. Se vaati nopeiden päätösten tekoa ja jatkuvaa toimenpiteiden vaikutuksien ja seurauksien arviointia. Valtakunnallisissa organisaatioissa se vaikeutti keskitettyä viestintää. Kriisi painotti joidenkin viranomaisten toimintaa tavanomaisesta poikkeavaan suuntaan. Toisaalta kriisi on tuonut sisäisesti eri sektoreita yhteen ja tekemään yhdessä operatiivisia linjauksia.
Harjoittelun ja suunnittelun merkitys	Pandemiaa seurannut kriisi korosti yleisen varautumisen ja suunnittelun tärkeyttä. Aiemmin kriisejä harjoitelleet organisaatiot ovat saaneet korkean koron harjoittelutoiminnalle. Mitä enemmän on harjoiteltu,

	suunniteltu ja kehitetty toimintamalleja, sitä valmiimpia ollaan seuraaviin poikkeusoloihin ja pystytään keskittymään vaikeissa tilanteissa esiin nouseviin ad hoc -asioihin.
Ihmisten henkilökohtainen digiloikka	Organisaatioiden ohella digiloikkalähtökohdat olivat yksittäisillä ihmisillä hyvin erilaiset. Yhteiskunnallisella tasolla tarvitaan ihmisten kouluttamista organisaatioiden lisäksi, sillä muuten on olemassa riski, että digiosaamista puuttuu. Asiakkaan näkökulmasta pandemia kehitti digialustoja, valmiuksia ja sote-palveluita. Kehittämis- ja palvelutoiminnassa vuorovaikutuksen osalta tunnistettiin fyysisten kohtaamisten konkreettiset edut.
Muut vaikutukset henkilökohtaiseen elämään	Pandemia on koetellut yhteiskunnan lisäksi yksittäisten ihmisten kriisinsietokykyä. Positiivisina asioina se on mahdollistanut uusia virtuaalipalveluita, muistuttanut käsienpesuhygieniasta ja tuttujen rutiinien tekemisen tärkeydestä.

2.3. LUOTTAMUS OSANA DIGITAALISTA TURVALLISUUTTA

Podcastissa kysyttiin vierailta heidän näkemyksestään luottamuksesta ja kuinka sitä voitaisiin ylläpitää ja kehittää digitaalisen turvallisuuden osalta. Vastauksista on koostettu seuraavan jaottelun mukaiset kokonaisuudet luottamuksen ulottuvuuksista osana digitaalista turvallisuutta.

Yhteiskunnallinen luottamus, joka kohdistuu instituutioihin ja organisaatioihin	Suomi on luottamusyhteiskunta, joka perustuu osaamiseen ja koulutukseen. Suomalaisten pitää pystyä luottamaan viranomaisten toimintaan ja tietoyhteiskunnan sähköisiin palveluihin, vaikka tietoja esimerkiksi käytetään yhteiskäytössä eri organisaatioissa ja palveluissa esiintyy välillä kapasiteettiongelmia. Luottamusta digitaaliseen palvelukanavaan ja asiointiin tulee vaalia virtuaalisessa digiyhteiskunnassa ja ylläpitää sama taso kuin fyysisessä maailmassa. Yhteiskunnallista luottamusta rakennetaan normaalioloissa, sitä testataan poikkeusoloissa ja se heijastuu kriisinsietokykyyn ja resilienssiin.
Luottamus turvallisuussektorilla	Luottamus on toiminnan ydin, pohja ja perusta turvallisuussektorilla. Sitä ei voi menettää kriittisissä palveluissa kertaakaan, joten yhteiskunnan ja yksittäisten toimijoiden on varjeltava sitä tarkoin. Luottamus on avainasemassa hybridi- ja kyberuhkien torjunnassa ja elintärkeiden toimintojen turvaamisessa. Turvallisuussektorin osalta tulee varjella myös luottamusta kansainvälisen järjestelmän turvallisuuteen. Turvallisuusluokitellun ja tiedustelutiedon osalta kansallinen edun arvioinnissa tulee tietyissä tilanteissa huomioida, että tiedon käsittelyssä vaakakupissa on myös toisten valtioiden luottamus Suomen valtioon.
Luottamus tietojärjestelmiin ja tiedon suojaamiseen	Luottamus ansaitaan laadukkailla ja digiturvallisilla palveluilla, eikä se synny tai pysy yllä ilman jatkuvaa työtä luottamuksen rakentamiseksi. Luottamuksen puute digiturvaan voi heikentää merkittävästi palvelun vaikuttavuutta ja laatua. Luottamuksen rakentaminen ja ylläpito vaatii osaamista sekä käytännön toimenpiteitä, kuten tarkastuslistoja ja riskienhallintaa. Luottamus ei kuitenkaan ole jatkuvaa hallintaa, kontrollia tai liiallista seurantaa, sillä koskaan ei voida saavuttaa 100 % turvallisuutta. Voidaan pyrkiä ainoastaan parhaimpaan mahdolliseen lopputulokseen ja vastuulliseen riskien ja uhkien tunnistamiseen. Luottamuksen tulee myös kohdistua järjestelmiin ja yhteistyötoimijoihin, ettei kehittämiseen muodostu pullonkaulaa.

Ihmisten välinen luottamus	Luottamus on tunne ja kokemus, joka on osittain näkymätöntä yhdessä pitävää liimaa. Muodostuu usein niin että tunnet toisen osapuolen ja muodostat henkilökohtaisen suhteen. Liittyy osaltaan kokemukseen, jossa toinen käyttäytyy sinun toiveittesi mukaan eikä aiheuta pettymystä tai tuota pahaa. Tämä kannustaa ja ylläpitää kykyä ja tahtoa toimia yhdessä ja pyrkiä hyvään lopputulokseen.
Verkoston sisäinen luottamus	Verkostomaisessa toiminnassa ja luottamusyhteisöissä, kuten valtioneuvosto tai poolitoiminta, korkea sisäinen luottamus on elintärkeää. Korkea luottamus mahdollistaa yhteistyön ja -toiminnan, jolloin yhdessä tekeminen ja esimerkiksi tutkimus johtaa parempaan lopputulokseen. Aidossa kumppanuudessa osoitetaan myös omat virheet ja kehityskohteet, joita voidaan yhdessä kehittää.
Luottamuksen ylläpidon keinot	Luottamusta instituutioihin, järjestelmiin ja ihmisiin voidaan ylläpitää karkeasti avoimuuden, rehellisyyden ja läpinäkyvyyden kautta. Avoimuutta tarvitaan niin toiminnasta, sen syistä kuin vaikuttavuudestakin. Esimerkiksi häiriö- ja poikkeamatilanteissa luottamuksen ylläpitämiseksi tulee tiedottaa avoimesti, kuten myös ennakoiden, esimerkiksi tietoturva-auditoinneista, jäännösriskeistä ja akkreditoinneista. Rehellisyys ja läpinäkyvyys sekä selkeäkielisyys vaikeista asioista mahdollistavat tietoturvan peruselementit ja mahdollisen julkisen kontrollin tai tarkastuksen kohdistamisen. Organisaation tulee olla sitoutunut luottamuksen rakentamiseen ja kehittämiseen ja sen tulisi olla yhteen lausuttu teema.
Yhteiskunnallisen luottamus poliittishallinnollinen ylläpito	Viranomaisten tulee vaalia luottamusta toiminnassaan noudattamalla oikeusvaltioperiaatetta, toimimalla lakien sekä asetusten mukaisesti sekä ehkäisemällä korruptiota. Viranomaisten tulee noudattaa hyvän hallinnon periaatteita ja taata esimerkiksi päätöksille valitusmahdollisuus. Päätöksenteossa ja lainsäädäntöprosessissa tulee ottaa huomioon erilaiset mielipiteet. Viranomaisten tulee huolehtia valvonta- ja tarkastustoiminnasta sekä toimintakertomuksien läpikäynnistä.
Luottamus kilpailuetuna	Suomeen on perustettu esimerkiksi hybridiuhkien osaamiskeskus, joka on osoitus siitä, että Suomeen ja suomalaisiin luotetaan digiturvan ja varautumisen kysymyksissä.

Luottamus maineen kaltaisena	Luottamuksen rakentaminen kestää pitkään ja sen voi menettää esimerkiksi tietojenkalastelutilanteissa hyvin helposti.
Luottamus yrityksiin	Yrityksiin kohdistuvan matalan luottamuksen osalta tunnistettu ero on, että julkisessa hallinnossa ollaan lähtökohtaisesti avoimempia verrattuna yrityksiin. Luottamuksen parantamiseen yrityksiin tulisi panostaa esimerkiksi kyberturvallisuuden kehittämisohjelmassa.
Pahantahtoinen luottamus	Luottamusta herättävä toiminta on päätöksenalainen asia. Pahantahtoiset tahot voivat käyttää luottamusta myös väärin ja tehdä huijausyrityksiä esimerkiksi poliisina. Siksi luottamuksen tueksi vaaditaan huolellisuutta digipalveluissa.

2.4. VINKIT HENKILÖKOHTAISEN ELÄMÄN DIGITAALISEEN TURVALLISUUTEEN

Podcastissa vierailta kartoitettiin heidän henkilökohtaisia toimintatapojaan, joilla he huolehtivat ennen kaikkea henkilökohtaisessa elämässään digitaalisesta turvallisuudesta. Podcast-vieraat painottivat vinkkeinä erityisesti oikeanlaista asennoitumista toimintaan digimaailmassa ja siellä kohdattaviin haasteisiin. Yksityiskohtaisemmin podcast-vieraat painottivat digiturvavinkeissä päätelaitteisiin ja sovelluksiin, tietoliikenneverkkoihin, fyysiseen ja sosiaaliseen ympäristöön, salasanoihin, tunnistautumiseen, tiedonhallintaan, asumiseen ja kodin laitteisiin liittyviä digiturvallisuusvinkkejä.

Ylätasolla podcast-vieraat erittelivät asennetta liittyen digimaailmassa toimimiseen ja operatiiviseen toimintatapaan digimaailmassa. Podcast-vieraat painottivat tarkkuutta ja kriittistä epäileväisyyttä digimaailmassa asiakkaana ja käyttäjänä. Vaikka kiire, stressi, palveluiden toteutus tai muut ärsykkeet häiritsevät, verkossa on hyvä olla pikemminkin varovainen ja tiedostaen arvioida tarkoitusperiä kuin yliaktiivinen. Hyvää toimintatapaa kuvattiin kuitenkin ennen kaikkea maalaisjärjen käytöksi. Samat perusvinkit digimaailmassa ovat pääosin päteneet myös koronatilanteessa.

Operatiivisella tasolla digimaailmassa tulisi panostaa ymmärryksen lisäämiseen. Digiturvalliset ohjeistukset ja toimintatavat on hyvä sisäistää ja niitä tulee noudattaa kurinalaisesti organisaatio- ja yksilötasolla. Toisaalta podcast-vieraat huomioivat, että digipalveluissa on aina olemassa tietynlainen riski, jota ei täysin voida poistaa, jolloin turvalliseen palvelun käyttöön kannustaminen on hyvä pitää merkittävässä roolissa. Tämä näkyy esimerkiksi sosiaalisen median palveluissa, missä passiivisuus ja itsekuri helpottavat turvallista käyttöä, mutta toisaalta suuri tietovuoto olisi merkittävä maineriski palveluille. Tiettyjä väestöryhmiä, kuten lapsia ja vanhuksia, tulee podcast-vieraiden mukaan henkilökohtaisessa elämässä eniten tuettua viestimään, käyttämään laitteita ja toimimaan epäselvissä digimaailman tilanteissa. Kehittämisessä pitää kuitenkin huomioida käyttäjän näkökulmasta, että liian vaikeat turvallisuusjärjestelyt tietyissä palveluissa lisäävät todennäköisyyttä käyttää helppokäyttöisempiä mutta samalla turvattomampia palveluita.

Tarkempiin vinkkeihin liittyen päätelaitteet, sovellukset ja reitittimet tulee pitää päivitettynä ja asetukset kohdillaan. Päivitykset voi myös asentaa itse, sillä päivityksissä voi olla tiettyjä virheitä, joita ei ole vielä korjattu, jos asennuttaa kaikki päivitykset automaattisesti heti kun ne julkaistaan. Myös virustorjunta ja palomuurit tulee pitää päivitettyinä ja tietoa tulisi käyttää vain luotetuissa ja suojatuissa ympäristöissä, kuten VPN-yhteydellä turvatulla etäyhteydellä tai muussa luotetussa ja suojatussa verkossa, sekä siirtää ja luovuttaa tietoja käyttäen salattuja verkkoyhteyksiä.

Tiedon suojaaminen on hyvä huomioida myös fyysisissä ja sosiaalisissa ympäristöissä. Kannettavissa tietokoneissa on hyvä käyttää näyttö- ja kamerasuojuksia sekä huolehtia tietokoneen vartioinnista julkisilla paikoilla. Myös keskusteluympäristö on huomioitava esimerkiksi ei-julkisten kokouksien osalta. Sovellusten osalta tulee huomioida, miten ne jakavat käyttäjän paikkatietoa ja mille osapuolille. Tiedonhallintaan liittyen tiedot on hyvä varmuuskopioida ja ryhmitellä, jolloin tietoja voidaan

tarvittaessa hajasijoittaa esimerkiksi eri sijainteihin. Tietojen osalta on hyvä huomioida niiden luottamuksellisuus ja huolehtia tietojen oikeanlaisesta hävittämisestä kaikista eri medioista joihin niitä on tallennettu.

Käyttäjän tulee huolehtia siitä, että käytetyt salasanat ovat vaatimustenmukaiset, eli riittävän pitkät, monimutkaiset ja eriävät eri palveluissa. Apuna tähän podcast-vieraat suosittelivat erilaisia salasananhallintaohjelmistoja. Tunnistautumiseen on hyvä suosia sähköistä tunnistautumista mahdollisesti kaksivaiheisena, vaikkakin niissä on huomioitava mitä tietoa palveluntarjoajalle luovuttaa. Henkilötunnusta ei tulisi käyttää tunnistautumismenetelmänä ja osa podcast-vieraista suositti, ettei tarpeettomasti tietoja kyseleviä tai puutteellisia tunnistautumisratkaisuja käyttäviä verkkopalveluita tulisi käyttää.

Asumisen turvallisuuden ja varautumisen osalta on hyvä tarkkailla esimerkiksi IoT-laitteiden kytkeytymistä verkkoon ja laitteiden tietoturvaa sekä päivitystiheyttä. Laitehankinnoissa voi ottaa huomioon laitteen mahdollisen tietoturvamerkin. Työ- ja kotilaitteet on hyvä pitää erillään, ja muistaa että työtehtävissä käytetään työnantajan suojattuja laitteita. Laitteiden osalta säteileviä laitteita ei voi viedä kaikkiin tapaamisiin.

Digitaalinen turvallisuus on osa laajempaa kokonaisturvallisuusajattelua. Myös vinkeissä painotettiin digiturvan lisäksi kattavaa oman elämän varautumis- ja turvallisuusajattelua. Tähän liittyvät esimerkiksi sähköntuotannon tarkkailu, erilaisten varajärjestelmien olemassaolo ja käyttö tarvittaessa sekä varautumisasennoituminen myös henkilökohtaisessa elämässä.