[äänite alkaa]

Tuija Kuusisto [00:00:01]: Hei, olen Tuija Kuusisto, toimin valtiovarainministeriössä tietohallintoneuvoksena.

Kimmo Rousku [00:00:07]: Ja minä olen Kimmo Rousku, toimin digi- ja väestötietovirastossa eli DVV:ssä vahtipääsihteerinä. Tuijan kanssa me molemmat tahdomme edistää julkisen hallinnon digiturvallisuutta ja sitä kautta luottamusta yhteiskunnassa ja Suomen kilpailukykyä.

Tuija Kuusisto [00:00:25]: Tässä Digiturvakompassi-sarjassa me tapaamme Kimmon kanssa julkisessa hallinnossa vaikuttavia henkilöitä. Mitä on turvallisuus digimaailmassa, mihin suuntaan digiturvaa pitäisi kehittää? Tässä joitakin kysymyksiä yhdessä pohdittaviksi.

Kimmo Rousku [00:00:41]: Ja että siis mikä ihmeen digiturva? Digitaalisen turvallisuuden avulla huolehditaan riskinhallinnasta sekä toiminnan jatkuvuudesta, tietoturvasta ja tietosuojasta sekä edistetään samalla kyberturvallisuutta. Digiturva huolehtii meidän kaikkien tarvitsemien digipalvelujen toimivuudesta ja isona kokonaisuutena myös koko Suomen kyvystä selvitä erilaisista digimaailman häiriöistä ja hyökkäyksistä.

Tuija Kuusisto [00:01:10]: Tänään vieraanamme on tietohallintojohtaja Ari Uusikartano ulkoministeriöstä. Hyvää iltapäivää, Ari ja sydämellisesti tervetuloa tähän meidän Digiturvakompassi-podcastiimme.

Ari Uusikartano [00:01:24]: Kiitos kovasti kutsusta ja valinnasta tähän vaikuttajien joukkoon. Teema on ajankohtainen ja mielenkiintoinen.

Tuija Kuusisto [00:01:46]: Olet täsmälleen oikeassa. Digitaalinen turvallisuus, tai kyberturvallisuus, sehän on viime aikoina noussut kansainvälisen politiikan areenalle ja jopa siis valtiojohtajien kansainväli-

ten huipputapaamisten agendalle. Kyberturvallisuudesta, kyberhyökkäyksistä, ja sitten erilaisista vastatoimista, niistä keskustellaan vilkkaasti sekä asiantuntijoiden kesken että sitten mediassa ja myös tosiaan täällä ihan huippuluokan poliittisessa päätöksenteossa, niin Euroopan unionin sisällä kuin muissa kansainvälisissä yhteistyökuvioissa. Miten tämä kehitys näkyy siellä teillä ulkoministeriössä, tietohallintojohtaja Ari Uusikartano?

Ari Uusikartano [00:02:29]: Se on kehityksenä näkynyt jo kohtuullisen pitkän aikaa, eli kuten tuossa kuvasit Tuija, niin kehityshän on vienyt kaarena siihen, että hyvinkin teknologiapainotteisesta asiasta on tullut osa, ja hyvin keskeinen osa, poliittista agendaa. Tämä tietenkin johtuu siitä, että tähän meidän analogisen maailmamme rinnalle on tämä digitaalisuus noussut entistä vahvemmin, ja sitä myöten myös sitten digitaaliset uhat. Että jos arvioidaan tilannetta 10-15 vuotta sitten, niin silloin näistä asioista keskusteltiin teknisillä foorumeilla, mutta nyt ne ovat osa, kuten sanottu, poliittista agendaa. Ulkoministeriössä se on tietysti näkynyt silläkin tavalla, että paitsi monen muun maan tavoin meillekin on jo aikanaan nimitetty kybersuurlähettiläs näillä foorumeilla viestiä viemään, niin meillä on myös nyt sitten hybridisuurlähettiläs, joka sitten taas laajemmin tarkastelee tätä kokonaisuutta, erityisesti liittyen hybridivaikuttamiseen. Eli EU-foorumeilla, ja myös tietysti muualla kansainvälisillä foorumeilla, asia on erittäin keskeinen.

Kimmo Rousku [00:03:53]: No mites sitten, kun jos ajatellaan digitaalista maailmaa yleensä, niin Suomihan on kokoaan merkittävästi suurempi ikään kuin digivaltiona, niin mites sitten tämä kybertoimintaulottuvuus ja kyberpolitiikka? Yleensä aina jos kysytään, että mitäköhän nuo muut ajattelevat meistä, niin minkälainen maine Suomella on tavallaan tässä kyberpolitiikan kentällä?

Ari Uusikartano [00:04:18]: Suomi nähdään, jos käytän vanhaa terminologiaa, niin puolueettomana toimijana hyvinkin monessa asiassa. Eli olemme toisaalta siinä maineessa, että meillä on osaamista ja olemme edistynyt toimija digitaalisessa maailmassa, mutta toisaalta sitten taas meillä on myös, kun on puhuttu muun muassa siitä, että tulisiko meidän millä tavalla olla enemmän omavarainen liittyen niihin teknologisiin ratkaisuihin, joita digitaalisen turvallisuuden luominen edellyttää, ja näiltä osin olemme jossain määrin jäljessä naapurimaatamme Ruotsiakin. Mutta kaiken kaikkiaan meidät nähdään avoimena ja reiluna pelurina, joka sitten osaa myös valita ehkä kumppaninsakin oikein.

Tuija Kuusisto [00:05:18]: Joo, se on kyllä meidän kansainvälisen yhteystyömme kannalta tärkeää, että meidät nähdään puolueettomana ja ehkä tällaisena neutraalina, kuitenkin osaavana toimijana täällä digitaalisen turvallisuuden alueella. Mutta miten jos tästä sitten kansainvälisistä politiikan kuvioista mennään lähemmäs tätä sinun työpöytääsi, Ari. Kun toimit tietohallintojohtajana ulkoministeriössä, niin minkälaisia digitaaliseen turvallisuuteen liittyviä asioita sinun tällä virtuaalisella työpöydälläsi liikkuu?

Ari Uusikartano [00:05:52]: Paitsi virtuaalisella niin myös ihan oikeallakin työpöydällä, kenellä nyt vielä tässä monitilassa työpöytä sattuu olemaan. Mutta kysymyksenä hyvä, koska nythän on, niin kuin hyvin tiedämme, eletty tällaista hyvin poikkeuksellista aikaa tämän pandemian myötä, ja sitä myötä olemme tulleet hyvin vankasti havaitsemaan sen, että käytettävyys on osa turvallisuutta. Meillä ulkoasiainhallinnossa erityinen huoli tietenkin on se, että kuinka takaamme sen, että meidän verkostomme pysyy pystyssä ja toimivana, varsinkin kun välillä on ollut hankalaa tai lähes mahdotonta tehdä korjaavia ja päivittäviä toimenpiteitä yleensä siihen tekniseen alustaan, jolla tämä meidän toimintakykymme lepää. Eli kun näistä perusasioista mennään eteenpäin, niin tietenkin se, että minkälaisilla välineillä sitten kyetään harjoittamaan riittävällä tasolla riittävän turvallista vuorovaikutusta tilanteessa, jossa ei ole mahdollista matkustaa, niin se on ollut hyvin keskeinen. Se on ollut hyvin keskeinen myös EU:ssa, eli kaikki nämä etäkokoustamiseen, turvalliseen etäkokoustamiseen, tiedonvaihtoon liittyvät hankkeet ja ratkaisut ovat saaneet aivan uutta vauhtia tässä tilanteessa. Ei voi sanoa, että myöskään maailman meno olisi kovasti rauhoittunut sitten, koska kun ollaan tällaisessa tilanteessa, jossa ollaan ehkä entistä haavoittuvampia juuri tästä syystä, mitä kuvasin, niin uhkatekijöiden määrä on jatkuvasti kasvanut. Myös hyökkäysten laatu on jossain määrin parantunut, eli kyllä tässä työpöydällä kaikenlaista riittää. Ja sitten on näitä isoja poikkeamia, eli kuten mediasta olette saaneet seurata, niin vaikka Kabulin prosessissa digitaalinen turvallisuus ei ollut ihan keskiössä, niin silläkin osaltaan tietenkin oli vaikutuksensa siihen, että kyettiin operaatio kuitenkin kohtuullisen menestyksekkäästi suorittamaan. Eli kaikenlaista tällaista pientä on tässä virtuaalipöydällä.

Kimmo Rousku [00:08:25]: Viranomaisten viestintä, valeuutiset, ja faktaperustainen viestintä herättävät voimakkaitakin näkemyksiä ja tunteita. Voisitko kertoa joitakin tällaisia käytännön esimerkkejä siitä, miten ulkoministeriön hallinnonalalla tietoja voidaan hyödyntää vahingollisessa tarkoituksessa teitä vastaan?

Ari Uusikartano [00:08:49]: Ensimmäisenä tulee tietenkin mieleen mainehaitta, eli jos jotain tietoa vuotaa, jonka ei pitäisi, niin tietohan on aina tulkinnanvaraista ja se on joku osakokonaisuus jostakin, harvoin täydellinen kuva. Tällöin paitsi hallinnonalaa niin myös koko Suomen hallintoa vastaan voidaan hyödyntää tällaisia ilmentymiä. Mutta jos mietitään tätä koko valeuutisten kokonaisuutta, johon olemme saaneet nyt tässä tutustua aika laajalti myös ajatellen pandemiaa, mutta yleensäkin tätä toimintaympäristöä, missä olemme, niin se on tehokas ase. Se on kohtuullisen edullinen ja aina löytyy joko hyötyjiä tai uskojia, jotka lähtevät tähän valeagendaan mukaan, ja näin ollen siihen ei oikeastaan ole muita keinoja, kuin pyrkiä tuottamaan ajantasaista ja oikeaa tietoa. Haasteena on, että ihmiset erilaisista inhimillisistä syistä haluavat, jotkut jopa haluavat uskoa, että "I want to believe", ja sitten sen kuplan sisään, joka on esimerkiksi valeuutisten perusteella ympärille luotu, on hyvin vaikea päästä. Tällainen medialukutaidon opettaminen, tässä iässä, niin voi olla haastavaa, mutta kaiken kaikkiaan meillä on hyvin rajallinen määrä keinoja kuinka voidaan sitten torjua sitä disinformaatiota, ja kyllä meillä siitä aika paljon kokemuksia on. En nyt suoranaisesti pysty sitten kohdentamaan sitä omaan hallinnonalaani, mutta esimerkkinä nyt tietenkin voidaan kertoa vaikka se, että nyt tähänkin Kabulin operaatioon liittyi disinformaatiota, joko tahtoen tai tahtomattaan sillä tavalla, että minkälaisia keinoja esimerkiksi Suomella tai Euroopan mailla on auttaa evakuoinnissa epätoivoisia ihmisiä. Kyllä siinä sitten joudutaan tasapainoilemaan sen suhteen, että mitä ihan oikeasti voidaan tehdä, ja mitkä sitten ovat ihan puhtaasti sellaisia keinoja, joita ei käytännössä ole olemassa, mutta joita jotkut tahot sitten viestittävät, että tällaisia voisi olla. Ne ovat aina ikäviä, koska siihen liittyy sitten hyvin syvällinen tällainen inhimillinen ulottuvuus. Eli hyvin laaja kenttähän tässä on, kun puhutaan disinformaatiosta ja kuinka siihen voidaan reagoida ja kuinka sitä voidaan torjua.

Tuija Kuusisto [00:11:46]: Kiitos Ari, nämähän ovat koskettavia esimerkkejä siitä, kuinka digitaalinen turvallisuus itse asiassa tulee meidän kaikkien lähelle ihan iholle asti. Kun sitten mietitään, että yksi mikä paljon useita ihmisiä on koskettanut myös se, tai sanotaanko organisaatioita, että on jouduttu näiden erilaisten kiristyshaittaohjelmien uhriksi nyt tässä viime aikoina, ja rikolliset sitten ovat niistä taloudellisesti hyötyneet. Mainitsit, että myös tästä luottamuksellisen tiedon vuotamisesta voi tulla mainehaittaa, sitä ehkä voidaan käyttää myös tällaisten kohdennettujen kyberhyökkäysten suunnittelussa. Ja ikävä kyllä nyt eri puolilla maailmaa ja täällä Suomessakin on tapahtunut aika selkeä muutos siinä, että näitä onnistuneita kyberhyökkäyksiä on aika paljon ja vaikutukset ovat laajoja. Mutta miten näet, että miten sitten ulkoministeriön tietohallintojohtajana on mahdollista tähän kehitykseen vaikuttaa, ja toisaalta miten tällä kyberturvallisuustilanteen globaalilla pahenemisella, niin mitä vaikutuksia tällä on ollut teidän toimintaanne ulkoministeriössä?

Ari Uusikartano [00:13:03]: Olen aina tavannut sanoa, että puolustajahan lähtee näissä asioissa takamatkalta, kun ollaan tilanteessa, jossa ollaan pakotettuja reagoimaan, ja tietenkin se proaktiivinen toiminta on yhtä lailla tärkeää, jolla sitten pyritään tekemään jos ei nyt mahdottomaksi niin ainakin jossain määrin hankalaksi se, että miten sisälle päästään ja sitä tietoa päästään laittomin keinoin etsimään. Olen ollut sitä mieltä pitkään, ja olen edelleenkin, että kannattaa olla pikkuisen erilainen kuin muut, ja tämä pohjautuu siihen ajattelumalliin, että hyökkääjä, joka pyrkii tunkeutumaan järjestelmiin, niin se hyökkäysmetodiikka on aina jonkunmoinen investointi. Jos kaikilla on sama suojaus, niin investointi on aika tehokas, jos yksi avain käy kaikkiin lukkoihin. Tässä mielessä olen ollut pakotettu olemaan jossain määrin eri mieltä muun muassa Valtorin uuden toimitusjohtajan kanssa, joka totesi, että kaikki munat samassa korissa on turvallinen ratkaisu. En täysin eri mieltä, koska totta kai, jos kaikki on keskitetty, niin sitä keskitettyä on jossain määrin helpompi turvata kuin hajautettua, mutta taas jos meillä on hallittu hajautus, jossa on erilaisia turvaamisen ratkaisuja, niin silloin se vahinko ei välttämättä ole niin suuri. Eli tämähän on tasapainoilua, se, että mitä meillä on resursseja, osaamista ja investointeja sijoittaa tähän turvaamiseen. Valitettavasti vaan näyttää siltä, että elämme tällaista epätasapainoista aikaa, eli meillä on hyvin kunnianhimoinen ja vauhdikaskin palvelujen ja toimintojen digitalisaatioon vievä agenda, mutta taas se toinen puoli, eli vastaavat investoinnit sen ympäristön turvaamiseen, eivät ole tasapainossa. Sen takia olen tästä kehityssuunnasta huolissani, ja toivottavasti nyt tässä seuraavassa budjettiriihessä esimerkiksi kyberturvallisuuden kehittämisohjelmaan ja muihin digitaalisen turvallisuuden kehittämisratkaisuihin on mahdollista saada rahoitusta, koska jos näin ei käy, niin menetetään paitsi luottamus, joka on iso juttu, niin myös sitten ehkä arkaluontoistakin tietoa, ja se on todellakin vaikea kysymys. Ymmärrän, että se ei ole niin näkyvää, kun rakennetaan turvallisuutta, kuin jos rakennetaan joku iso palvelukonsepti ja kokonaisuus, joka sitten voidaan todeta, että tässä tämä hoituu sähköisesti ja säästetään kustannuksissa. En nyt halua sitä Vastaamo-keissiä nostaa niin esille, eikä se ole hyvä esimerkkikään tässä yhteydessä, koska suojaus oli niin alkeellinen siinä ympäristössä, mutta tämä on mielestäni valitettava epätasapaino, joka meillä nyt tähän hallinnonkin kehittämiseen kytkeytyy. Eikä ainoastaan hallinnon, vaan yleensäkin jos ajatellaan digitaalista yhteiskuntaa, niin kyllä siihen pitäisi merkittävästi enemmän panostaa siihen turvaamispuoleen.

Kimmo Rousku [00:16:30]: Tämä oli todella painokas kokonaisuus, jonka toit tuossa ehdottomasti esille, nimenomaan tämä näkymättömyys. Eli kun nämä asiat, joita me edistämme, ovat usein näkymättömiä, ne näkyvät vasta siinä vaiheessa, kun ne pettävät, jonka jälkeen yleensä sitten tulee niitä resursseja korjata asioita. Mutta nostit tuossa loistavasti esille tämän luottamuksen, että sehän on se tehtävä, jonka ylläpito ja kehittäminen ja säilyttäminen meillä kaikilla täällä on koko ajan käsillä. Meillä on toteutettu DVV:ssä näitä digibarometrikyselyitä, niin meillä on vielä kuitenkin aika hyvä luottamus, vastaajista noin 80% luottaa viranomaisiin, omaan työnantajaan, yrityksiin selvästi kuitenkin vähemmän. Mitä sinun mielestäsi, Ari Uusikartano, luottamus on?

Ari Uusikartano [00:17:21]: Luottamus on tietenkin, jos vähän yksinkertaistaa, niin ennen kaikkea läpinäkyvyyttä siihen, että voi luoda itse sen ymmärryksen, onko joku asia luottamuksen arvoinen vai ei. Tämä on vähän vaikea kysymys, koska kun puhutaan teknisistä asioista niin harvapa meistä kykenee sitten sen läpinäkyvyyden läpi käymään sillä tavalla, että voimme todellakin luottaa. Mutta miten ulkoasiainhallinnossa tätä asiaa on lähestytty, niin meillähän on pyritty viemään meidän turvallisuusratkaisumme jonkun standardin mukaiseksi, eli meille viime vuonna myönnettiin ISO 27001 -sertifikaatti ministeriön tietoturvatoiminnoille, joka osaltaan kertoo, sekä meille itsellemme toki mutta myös yhteistyökumppaneille, että se luottamus on jotenkin mitattavissa, ja sertifikaatti voi olla sellainen mittari ja soisi, että asioita vietäisiin tähän suuntaan. Luottamusta sitten esimerkiksi järjestelmätoimittajatahoihin voidaan rakentaa erilaisin sopimuksin, joiden pohjalta voidaan tehdä arviointeja ja auditointeja. Aivan samoinhan kansainväliset yhteisöt, Euroopan unioni, NATO, arvioivat, kuinka turvallista meille esimerkiksi on luovuttaa jotain tietoa. Eli siihen liittyvät sitten erilaiset tarkastuskäynnit auditointeineen, että sitä käsitellään sovitulla tavalla. Kun puhutaan tiedosta, jota digitaalisesti käsitellään, niin tiedon omistajahan määrittelee sen tavan, kuinka esimerkiksi sitä tietoa tulee turvata. Ja sitten sen tavan verifiointi luo luottamusta osaltaan. Tämä nyt vain yksi kapea kaistale tästä luottamuskysymyksestä, mutta tämähän on osa sitä kontrollia, ja kuten oppi-isämme Lenin on todennut, niin luottamus hyvä, kontrolli parempi. Ja tässä sitä voidaan nyt käyttää vähän positiivisemmassa mielessä, kun pelkästään hän sitä ilmeisesti ajatteli kansalaisen kontrolliin. Ja kyllä meidän täytyy se luottamus luoda senkin takia, tai siihen panostaa senkin takia, että nyt kun pyritään esimerkiksi tiedon käsittelyn automatisointiin entistä enemmän ja esimerkiksi automaattisen päätöksenteon tuomista mukaan, niin ei sitä tekoälyä voida päästää päättämään, jos ei luottamusta luoda esimerkiksi sillä tavalla, että me tiedämme, että kuka sitten lopulta vastaa, jos päätös olikin väärä. Me emme voi syyttää sitä algoritmia. Eli tämä on iso kysymys, ja tämä on erityisesti säädösnäkökulmasta merkittävä asia, eettis-moraaliseltakin kannalta, kun mietitään, että mihin teknologia toisaalta luo mahdollisuudet, mutta minkälaiset kontrollit siihen täytyy sitten kyetä luomaan.

Tuija Kuusisto [00:20:25]: Mitenkäs sitten, jos lopuksi viimeisessä kysymyksessä mennään ihan omaan elämääsi ja miten omassa elämässäsi huolehdit digitaalisesta turvallisuudesta, niin minkälaisia vinkkejä sinulla Ari olisi meille kaikille?

Ari Uusikartano [00:20:42]: Taidan olla jossain määrin valitettavan lepsu tai perinteinen turvaamisratkaisuissani, ja käytän toki teknologiaa kohtuullisen sujuvasti ja tuen myös perhepiirissä näissä asioissa,

joissa toisaalta tuntuu, että lapset ovat paljon fiksumpia kuin meikäläinen, mutta perustoimenpiteet toki laitteiden suojaaminen, salasanakäytänteet vastaavat, niin niihin täytyy tietenkin satsata. Erityisesti jos ajattelee itseä niin täytyy pyrkiä pysymään ajan tasalla että missä mennään, koska kun nyt tälläkin sektorilla on toiminut jo vuosikymmeniä erilaisissa tietohallintoon, tiedon hallintaan ja turvallisuuteen liittyvissä tehtävissä, niin kyllä kehitystyö on jatkuvaa, ja jos ei siinä edes rinnalla juokse niin aika pahasti jää jälkeen. Mutta en nyt voi sanoa, että olisin mitenkään erityisen innovatiivinen näissä turvaamisasioissa, eli luotan siihen, että minulla on sitten osaavia ihmisiä, joko meillä töissä tai jotka tunnen, joiden konsultaatiota voin käyttää. Eli kyllä se asia paremminkin voisi olla, mutta en nyt kuitenkaan henkilökohtaisessa elämässäni ole vielä joutunut esimerkiksi kiristyshaittaohjelman uhriksi tai vastaavaan tilanteeseen, jossa tietojani olisi lukittu. Että hyvin on mennyt, mutta toisaalta pitää aina koputtaa sitä maalaamatonta puuta, että toivottavasti menee jatkossakin, koska tämä nyt vaan tämä tilanne ilmeisesti tulee olemaan hankala ja ei mitenkään helpottamaan, ja kun katsoo näitä viimeisiä, tai viimeisimpiä sisällepääsy-yrityksiä, niin voi todeta, ettei enää suomen kielikään meitä kovin hyvin suojaa. Että kyllä nuo joko käännösrobotit tai pahantahtoisten tahojen palveluksessa olevat ihan kansalliskielisetkin kykenevät luomaan ihan uskottavia viestejä, joilla pyritään kalastelemaan meiltä pankkisalaisuuksia ja muita tunnuksia tai yleensä tietoa. Eli maailma on paha, mutta yhteistyössä me siitä selviämme.

Tuija Kuusisto [00:23:03]: Kyllä, tähän on hyvä lopettaa, yhteistyössä on voimaa. Kiitos Ari Uusikartano haastattelusta.

Kimmo Rousku [00:23:10]: Kiitos.

Ari Uusikartano [00:23:10]: Kiitos.

[äänite päättyy]