[äänite alkaa]

Tuija Kuusisto [00:00:01]: Hei, olen Tuija Kuusisto.

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.

Kimmo Rousku [00:00:38]: Mikä on digiturva? Digitaalisen turvallisuuden avulla huolehditaan riskienhallinnasta ja toiminnan jatkuvuudesta, tietoturvasta ja tietosuojasta, sekä edistetään kyberturvallisuutta. Digiturva huolehtii meidän kaikkien tarvitsemien palveluiden toimivuudesta, ja isona kokonaisuutena myös koko Suomen kyvystä selvitä erilaisista digimaailman häiriöistä ja hyökkäyksistä.

Tuija Kuusisto [00:01:02]: Tänään meidän podcastimme vieraana on kansallisen turvallisuuden yksikön johtaja, Petri Knape sisäministeriöstä. Hyvää iltapäivää Petri, ja sydämellisesti tervetuloa tähän Kimmon ja minun podcastiimme.

Petri Knape[00:01:17]: Hyvää iltapäivää Tuija ja Kimmo, ja kiitos paljon että pääsin mukaan tähän teidän podcastiinne. Mukava olla keskustelemassa tärkeistä turvallisuusasioista.

[musiikkia 00:01:26]

Tuija Kuusisto [00:01:43]: Petri, sinä toimit kansallisen turvallisuuden yksikön johtajana, ja sisäministeriössä. Mikä on näkökulmasi, mitä kansallinen turvallisuus oikein tarkoittaa?

Petri Knape[00:01:57]: Tämä on oikeastaan hyvä kysymys. Kansallinen turvallisuus sinänsä terminä on melko uusi, se lanseerattiin suomalaiseen lainsäädäntöön siviili- ja sotilastiedustelulakien säätämisten myötä. Tarkemmin sitä pohdittiin sisällöllisesti perustuslaki kymmenennen pykälän muuttamisen valmisteluasiakirjoissa. Ytimeltään voisi sanoa niin, että kansallisen turvallisuuden eksakti määritelmä on vaikeaa, tai jopa mahdotonta tehdä. Kansallinen turvallisuus elää ajassa. Sitä voidaan arvioida, siihen kohdistuvien uhkien kautta. Ja sen ytimessä on kansakunnan, eli tässä tilanteessa Suomen, itsenäisyys ja suvereniteetti. Joka voi vaarantua useilla eri tavoille, useiden eri toimijoiden toimesta.

Määrittelyä on moneen kertaan peräänkuulutettu, mutta olen itse kyllä vakuuttunut siitä, että tietynlaisten peruspilareiden, uhkien, tunnistaminen on olennaista tässä. Ja sen kansallisen turvallisuuden ydin elää itse asiassa turvallisuusympäristön muutosten kautta.

Kimmo Rousku [00:03:06]: Globaalisti, ja Suomi edelläkävijänä ennen kaikkea, digitalisoituminen leviää kaikilla eri yhteiskunnan toiminnan alueilla. Nyt koronapandemia on voimakkaasti vauhdittanut tätä digitalisoitumista. Viranomaisten kanssa asiointi, kuten passin hakeminen, verkko-ostokset, ja nykyisin myös etämatkailu ja erilaiset etätapahtumat, sekä toki esimerkiksi tavanomainen toimistotyöskentely, tämä kaikki on siirtynyt verkkoon. Mikä kansallisen turvallisuuden näkökulmasta on keskeistä tämän digitaalisen ympäristömme turvallisuudessa, eli digiturvallisuudessa?

Petri Knape[00:03:43]: Lähestyisin tätä kysymystä ja pohdintaa kolmesta eri aspektista. Ja tietenkin kansallisen turvallisuuden tulokulmalla. Mutta ensin muutama sana tästä pandemiarajoitusten aiheuttamasta etätyöskentelyn räjähdysmäisestä lisääntymisestä. Sitten luonnollisesti meidän teknologinen kehityksemme, jossa yhteiskunta digitalisoituu kovaa vauhtia. Ja kolmantena pointtina erityisesti kansallisen turvallisuuden näkökulmasta on syytä mainita valtiolliset kybervakoilutapaukset, joita Suomenkin osalta on julkisuuteen tullut, ja joita maailmalla aika ajoin, enenevissä määrin, ja vakavuudeltaan haasteellisempia tapauksia tulee ilmi. Mutta nyt jos menemme tähän etätyöskentelyn merkittävään kasvuun, joka todennäköisesti tulee myös jäämään pysyväksi ilmiöksi. Ei ehkä samalla volyymilla jolla yhteiskunta sitä nyt tekee, mutta jatkossa todennäköisesti enemmän kuin mitä ihmiset aiemmin ovat tehneet. Olennaistahan on, että näissä tilanteissa kansalaiset, työntekijät, virkamiehet, jotka istuvat toimistojen sijasta kotikonttoreissaan, niin heidän täytyy pystyä luottamaan siihen viestintäverkkoon, ja viestintävälineisiin, joita työn tekemiseen käytetään. Tässä suhteessa kansallisen turvallisuuden näkökulmasta ehkä olennaisinta on se, että meillä Suomessa verkkoturvallisuus on erittäin hyvällä tasolla. Mutta reilu vuosi sitten säädettiin muutokset tuohon sähköisen viestinnän palvelulakiin. Ja sinne saatiin säännökset, joilla ennakkoon halutaan estää se, että verkkojen kriittisiin osiin sijoitettaisiin sellaisia viestintäverkkolaitteita, joiden osalta on perusteltua epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta. Ja tämä mahdollistaa niihin puuttumisen. Ja riippuen tilanteista, niin tällaisessa tilanteessa voidaan puhua myös niin sanotusta laitetoimittajariskistä. Ja tämä kytkeytyy myös eurooppalaiseen keskusteluun. Tämä on ehkä verkkojen toimivuuden ja kansallisen turvallisuuden kannalta se oleellinen tekijä. Toinen teema jonka halusin ottaa esille on tämä meidän voimakas teknologinen kehittyminen. Arjen toimintojen siirtyminen verkkoon yhä enenevissä määrin. Näin ATK-ajan ihmisenäkin voin todeta, että ilmeisesti 5G sitä erityisesti tulee tuomaan mukanaan, jääkaapeista lähtien. Mutta tämä digitaalinen kehittyminen ja teknologinen murros ulottuu myös olennaisesti meidän kriittiseen infrastruktuuriin Suomen valtiossa. Ja näin ollen meidän energiatoimintomme, vesihuoltomme, logistiikkaketjumme, ja niin edelleen, jotka takaavat että yhteiskunta toimii, ovat hyvin tiiviisti kytkennässä siihen, että millä tavoin verkon kautta niitä

etäohjataan, ja miten ylipäänsä se järjestelmä toimii. Tämä digitaalinen kehitys tuo luonnollisesti joustavuutta ja tehokkuutta meidän jokaisen arkeen, kunhan vain jaksamme itse pysyä mukana siinä tehokkuudessa. Mutta kolikon toinen puoli on tietenkin se, että se luo automaattisesti myös uusia haavoittuvuuksia erilaisille kyberhyökkäyksille. Ja näissä tilanteissa sitten yhteiskunta voidaan melko helposti jopa lamaannuttaa verkkojen kautta, ilman että perinteisellä tavalla edes yhteiskunnan turvallisuutta vakavasti uhattaisiin. Ajankohtainen esimerkki ehkä tuo Yhdysvalloissa tapahtunut Colonial Pipelinen tietomurto, joka siellä johti vakaviin muutoksiin, jopa polttoainetoimitusjärjestelmien keskeyttämiseen. Tämän tapaisten toimintojen takana voi olla vihamielisiä valtioita, tai sitten jopa kyberrikollisia, kiristäjiä, useita eri toimijoita. Viimeisenä pointtina nämä ikävät valtiolliset verkkorikostapaukset, joiden osalta Suomikaan ei ole ollut turvassa. Ja niissä samanlainen toimintamalli, kynnys verkkoja pitkin tunkeutua toisten valtioiden keskeisiin tietojärjestelmiin, hankkia sieltä sellaista tietoa, joka vahingoittaa sitä kohdevaltiota, ne ovat valitettavasti lisääntyneet, ja myös Suomeen on kohdistunut tällaista toimintaa. Kytkennässä meidän ulkoturvallisuuspoliittiseen päätöksentekoon, maanpuolustukseen, ja suomalaiseen huippututkimukseen. Ja nämä kaikki osaltaan myös vaikuttavat meidän kansalliseen turvallisuuteemme. Tähän on syytä jatkossa kiinnittää huomiota. Mutta nämä kolme elementtiä nostaisin tässä esiin.

Tuija Kuusisto [00:08:34]: Kiitos Petri. Ja kuten selkeästi toitkin esille, niin nämä erilaiset uhat ovat nyt viime aikoina valitettavasti realisoituneet maailmalla. Ja osin täällä Suomessakin. Emme tiedäkään julkisuudessa, kuinka paljon mahdollisesti näitä tietoturvaloukkauksia ja kyberhyökkäyksiä on pystytty estämään, ja kuinka paljon on sitten niiden vaikutuksia pystytty rajaamaan ja minimoimaan sitä, millaista vahinkoa ne ovat meidän yhteiskunnallemme aiheuttaneet. Tässä suhteessa kyllä luotan, että sisäministeriössä on tehty paljon töitä, joista ei tietenkään julkisuudessa voi kertoakaan. Mutta kuten totesit, näitä tietoturvaloukkauksia ja kyberhyökkäyksiä vaikuttaisi olevan yhä enemmän, ja näitä onnistuneitakin hyökkäyksiä on ollut myös Suomessa. Kuinka näet kehityssuunnan olevan tulevaisuudessa? Olemmeko menossa yhä vaikeampia aikoja kohti, vai näetkö mahdollisesti valoa tässä suhteessa, että voisiko tilanne kääntyä parempaan? Miten näitä erilaisia tulevaisuuden uhkia ja riskejä sitten punnitaan sisäministeriössä, ja minkälaista toimintaa se mahdollisesti teillä on aiheuttanut, tai tulee aiheuttamaan?

Petri Knape[00:10:00]: Tämä on tietenkin hyvä kysymys tarkastella. Ja itse oma taustani turvallisuusviranomaisten erilaisissa tehtävissä neljän vuosikymmenen aikana, itse asiassa viiden vuosikymmenen aikana pian olleena, niin näkisin kuitenkin niin, että kyllä hyökkäysjärjestelmät kehittyvät, koko ajan tulee uusia tapoja tehdä rikoksia tai loukata kansallista turvallisuutta, uhata sitä. Samaan aikaan kuitenkin myös puolustukselliset toimenpiteet, suojausjärjestelmät, kehittyvät. Mutta se menee aina niin päin, että tulee uusi tapa tehdä rikoksia, tai uhata kansallisturvallisuutta, tietoturvallisuutta, ja turvajärjestelmät tulevat perässä. Tässä suhteessa tällainen tasapaino nähdäkseni

tulee kuitenkin pitkässä juoksussa säilymään. Ja omasta näkökulmastani tietenkin en halua olla kyynikko, mutta uskon niin, että tietty määrä oikeuden loukkauksia ja tietomurtoja on osa arkea yhteiskunnissa. Niitä ei tietenkään pidä hyväksyä, mutta 100 prosenttisesti niistä ei koskaan tulla pääsemään pois. Teemme kaikkemme, että ne ovat minimaalisia, ja että niiden vaikutukset ovat mahdollisimman vähäisiä. Mutta sellaiseen utopiaan, että sellaisia uhkia ja tekoja ei lainkaan olisi, niin mielestäni siihenkään ei kannata tuudittautua, tai sitä ei ehdottomana kannata tavoitella. Tietenkin tähän myös vaikuttaa moninainen keskinäisriippuvuus. Yhteiskuntahan digitalisoituu voimakkaasti, kuten tuossa alussa sanoin. Ja tämä kybermaailma tai digimaailma, sen sovittaminen meidän perinteiseen tapaamme hahmottaa arkea ja valtionhallintoa, Suomen yhteiskunnan toimintaa, on haasteellista. Koska näkisin itse sen niin, että meillä on perinteisesti ajateltu yritysmaailmassa tai valtionhallinnossa, menemme toimialakohtaiseen niin sanotusti vertikaaliseen lähestymistapaan. Puhumme puolustushallinnosta, sisäasiahallinnosta, ulkoasiahallinnosta, pankkimaailmasta, vakuutusmaailmasta, puuteollisuudesta, niin edelleen. Kyber itse asiassa ulottuu näihin kaikkiin. Ja kyber yritetään helposti, ja digiturvallisuus sovittaa yhdeksi perinteiseksi vertikaaliseksi toimialaksi lisää sinne. Mutta kyseessähän on itse asiassa horisontaalinen kaikkiin ulottuva toimisektori. Ja näin ollen tämä monialaisuus asettaa myös suuria haasteita, että miten digitaalisesta turvallisuudesta voidaan hyvin pitää parhaalla mahdollisella tavalla huolta. Ja nostaisin tässä yhteydessä keskiöön sen, että meidän pitäisi löytää tämän perinteisen toimiala- ja sektorikohtaisen lähestymistavan rinnalle sellainen tapa, jossa meillä on yhteinen reaaliaikainen jaettu tilannekuva vakavimmista digimaailman uhista. Ja sen yhteisen tilannekuvan perusteella pystytään nopeasti ratkaisemaan se, että kuka tai ketkä ryhtyvät sitä kulloinkin esille nousevaa tapausta selvittämään toimivaltuuksiensa puitteissa. Ja tämän näkisin keskeisenä haasteena, että tämän tyylinen uusi tapa toimia tiiviisti yhdessä voisi levitä, ja siitä löydettäisiin toimivia ratkaisuja. Jolla sitten tähänkin lähestymistapaan luonnollisesti kytkeytyvät haasteet kyetään ratkaisemaan. Mutta töitä luultavasti tämän asian tiimoilta tehdään. Sisäministeriö yhtenä toimijana on mielellään mukana näissä keskusteluissa.

Kimmo Rousku [00:13:51]: Tässä on noussut jo erinomaisesti esiin se, että digitalisaatio tarjoaa aivan loistavia mahdollisuuksia. Ja on valotettu myös tähän liittyviä uhkia. Viestintä yleensäkin, erityisesti viranomaisten viestintä, siihen liittyvät valeuutiset, tutkimustiedon merkitys. Nämä herättävät voimakkaitakin näkemyksiä, myös sosiaalisessa mediassa ja muualla. Voisitko jollain lailla havainnollistaa ja kertoa joitakin käytännön esimerkkejä esimerkiksi siitä, kuinka valeuutisia voisi tunnistaa? Tai muita omia havaintojasi tähän kokonaisuuteen liittyen?

Petri Knape[00:14:31]: Valeuutiset ja informaatiovaikuttaminen ovat myös tämän päivän tapoja vaikuttaa yhteiskuntien toimintaan. Ja ainakin välillisesti vaikuttaa myös kansallisen turvallisuuden kysymyksiin, tai yhteiskunnan kykyyn vastata niihin. Ja olennaista ehkä valeuutisten osalta on, että onnistuakseen ne edellyttävät otollisen maaperän, eli niillä tulee olla jonkinlainen uskottava

kuulijakunta, joka ottaa ne totena, ei kyseenalaista niitä, ja ryhtyy hahmottamaan ympäröivää maailmaa niiden kautta. Tässä suhteessa voisi ehkä mainita esimerkkinä vuodelta 2016 USA:n presidentinvaalien ajalta Pizza Gate -tapauksen, jossa Donald Trump ja Hillary Clinton lähtivät repimään vaalikamppailua. Ja silloin amerikkalaisen äärioikeiston käyttämillä keskustelupalstoilla alkoi levitä huhu Washingtonissa sijaitsevasta pizzeriasta, josta käsin väitettiin Clintonia johtavien demokraattien pyörittävän kansainvälistä lapsikauppaliigaa. Ja tämä uutisointihan levisi sitten, ja sitä myös levitettiin aktiivisesti Twitteriin ja Facebookiin. Ja sosiaalisen median kautta sitä tukivat myös vieraan valtion järjestelmät ja toimijat, joilla oli intressiä boostata tätä valeuutiskampanjaa. Ja se levisi myös sitten Trumpin kampanjatiimin. Lopputuloksenahan tällä ikävällä tapauksella oli se, että näihin valeuutisiin vahvasti uskonut kahden lapsen isä tunkeutui pizzeriaan puoliautomaattikiväärin kanssa, ja tarkoitus oli surmata tämän kuvitellun lapsikauppaliigan pizzerian kellarissa piileskelevät jäsenet. Onneksi sieltä kellarista ei ketään löytynyt, ja tekijä antautui sitten poliisille, ja kukaan ei saanut surmaansa. Mutta tämä ehkä kuvaa pahimmillaan sen, mitä kaikkea voi tapahtua silloin, jos valeuutiset uppoaa otolliseen maaperään. Oikeastaan keskeisiä asioita sen tunnistamiseen ovat luultavasti valistunut median käyttäminen ja kriittisyys median uutisointiin, uutisten laatuun, tapaan millä niitä esitetään, minkä välineiden kautta niitä esitetään. Kuka se taho on, joka niitä esittää. Millainen sosiaalisen median jälki esimerkiksi tuolla eri kanavilla tällä kyseisellä uutisten levittäjällä on. Vastaavasti jos joku haluaa taas valeuutisista tehdä uskottavampia, niin montaa näistä elementeistä voidaan myös sitten häivyttää ja vaikeuttaa sillä tavoin uutisten tunnistamista. Mutta yleisesti uskon että Suomessa ollaan hyvin tietoisia ja kriittisiä median osalta. Vakavimpiin valeuutiskampanjoihin mukaan lähteminen, pitäisin sitä kuitenkin melko pienenä todennäköisyytenä. Vaikkakin nyt esimerkiksi tämän koronapandemian aikana on ollut myös esimerkkejä siitä, että jotkut valeuutisina pidettävät kampanjat ovat kuitenkin saaneet kannatusta yhteiskunnassa.

Tuija Kuusisto [00:17:46]: Mainitsit Petri aikaisemmin, että tarvitsemme kaikkien viranomaisten yhteistä jaettua tilannekuvaa digitalisoitumisesta ja sen turvallisuudesta, jotta kykenemme sitten yhteiskuntaa suojaamaan viranomaistoimin. Miten näet, että tähän tilannekuvaan saadaan sitten niitä niin sanottuja oikeita tietoja siitä, mitä on tapahtunut, tapahtumassa, ja miten ennakoida mitä tulevaisuudessa tulee tapahtumaan. Näetkö, että siellä on mahdollista, että sitä tilannekuvaa häiritään jonkinlaisilla valetiedoilla? Tai kun monessa asiassa on niin, että meidän ymmärryksemme ja tieto karttuvat matkan varrella, niin ehkä joudumme joissain tilanteissa toimimaan ennen kuin on vielä sitä riittävää kokonaiskuvaa olemassa. Sehän on nähty tässä pandemiassakin, että meidän käsityksemme koronasta on muuttunut koko tämän puolentoista vuoden aikana. Samahan tapahtuu siellä kyberuhkien maailmassa. Miten voimme varmistua, että viranomaisten tilannekuva säilyisi sitten mahdollisimman vankalla pohjalla?

Petri Knape[00:19:00]: Tämä on erittäin hyvä kysymys. Ja todellakin tuo mitä kerroin tuosta yhteisestä reaaliaikaisesta jaetusta tilannekuvasta, niin sehän on hyvin alkutekijöissään oleva ajatus ja idea siitä, mitä kannattaa tavoitella. Ja siihen sisältyy luonnollisesti paljon heikkoja tai korjattavia kohtia, jotka edellyttävät miettimistä, että mitä niissä on tehtävissä. Lähtökohtaisesti on itsestään selvää, kuten jo viittasinkin, että digimaailman ja kybermaailman luonteeseen kuuluu että ne kattavat niin suuren osan yhteiskunnan toimintaa, että sellainen utopia siitä, että tilannekuva kattaisi kaikki sektorit, tai siellä havaittaisiin kaikki, niin sellainen ei ole mahdollista. Puhumattakaan, että se voisi olla yhden tahon hallussa. Yksi virasto tai ihminen voisi sen tehdä. Kyllä tästä täytyy löytää ratkaisuja sellaisesta verkostomaisesta toimintatavasta, jossa kyetään myös suodattamaan niiden vakavimpiin uhkiin viittaavien tilannekuvaelementtien edelleen välittäminen oman asiantuntemuksen kautta. Mutta kuten sanoin, niin tämän tyylinen ajatus, mikäli sitä pidetään laajemminkin tarpeellisena, se vaatii luonnollisesti hyvää ja huolellista valmistelua. Ja kuten totesin, uudenlaista lähestymistapaa myös siihen, että miten nämä ratkaisut ovat tehtävissä. Meillä maailmalla joitakin esimerkkejä tällaisesta toimintatavasta on, mutta niistä tietenkin suorien johtopäätöksien vetäminen on vaikeaa. Enkä haluaisi missään nimessä tässä haastattelussa mennä sen syvemmälle, koska ei minulla missään nimessä ole suoria vastauksia niihin lukuisiin kysymyksiin, joihin vastaukset edellyttävät tällaisen toimintamallin tavoittelun ylipäänsä.

Tuija Kuusisto [00:20:50]: Kiitos [?? 00:20:50], oikein paljon mietteitä herättäviä ajatuksia siitä, että on lähtökohta että yhdessä tekemällä saadaan aikaiseksi enemmän. Se on luultavasti tässäkin se hyvä perusta. Ja turvallisuuden yhteydessähän puhutaan paljon luottamuksesta. Ja kun tässä on tehty näitä digiturva-barometrejä, niin on todettu, että noin 80 prosenttia vastaajista luottaa siihen, että viranomaiset käsittelevät turvallisesti ihmisten henkilötietoja ja muita tietoja, mutta yrityksiin luottaa ainoastaan 27 prosenttia. Miten näet, yksikön johtaja Petri Knape, mitä on luottamus?

Petri Knape[00:21:30]: Mielenkiintoisia lukuja kaiken kaikkiaan. Luottamushan on oikeastaan kaikenlaisen yhdessä toimimisen ydin. Ja sitä voidaan arvioida kansalaisten suhteessa valtiovaltaan, kansalaisten suhteessa viranomaisiin, ja kuten tässä oli, kansalaisten suhteessa yrityksiin. En osaa lonkalta arvioida, miksi tuo luottamus yrityksiin on noin alhainen. Suomessahan perinteisesti viranomaisiin luotetaan hyvin korkeilla prosenteilla. Siihen luultavasti myös historialliset syyt vaikuttavat. Luottamus on turvallisen yhteiskunnan ytimessä, ja pitäisin sitä asiana, jota ainakin viranomaisten on syytä vaalia huolella. Ja se luottamus ansaitaan arjessa joka päivä, itse asiassa uudestaan. Ja se ansaitaan tekojen kautta, ei sanojen kautta. Ja luottamus kun on kerran menetetty, niin sen takaisin saaminen on erittäin haastavaa. Kaiken kaikkiaan luottamus on turvallisuuden ytimessä, ja se on myös yhteiskunnan toimivuuden ytimessä. Sen vuoksi siitä on syytä pitää hyvin tarkalla kädellä huolta.

Kimmo Rousku [00:22:54]: Tuossa aikaisemmin nostimme esille sen, että tämä uhkatilanne on muuttumassa yhä enemmän kyberhyökkäyksiksi, ja muihin digitaalisen maailman ikäviin asioihin, joita tapahtuu onnistuneesti. Mitkä olisivat keinoja, joilla voisimme kansalaisten luottamusta vahvistaa, tai edes ylläpitää tällaisella nykyisellä tasolla?

Petri Knape[00:23:18]: Kyllä kuten äsken totesin, niin se hankitaan arjessa ja tekojen kautta. Ja tässä suhteessa avoin viestintä nousee myös keskeiseen rooliin.[?? 00:23:29] viestintä ei aina kaikissa kohdin voi olla täysin avointa, kuten tuossa aiemmankin keskustelun yhteydessä kävi ilmi. Mutta niin pitkälle avointa kuin se suinkin on mahdollista. Ja samaan aikaan rehellistä ja luotettavaa. Jos jokin asia on mennyt pieleen, niin on parempi se kertoa saman tien, ja tuoda sen jälkeen esille korjaavat toimenpiteet. Nämä ovat nähdäkseni keskeisiä keinoja, joilla luottamusta voidaan lisätä. Ja sen epäilyksen syntyminen tapahtuu hyvin herkästi, ja sitä kautta ollaan kaltevalla pinnalla. Avoin, rehellinen, oikea-aikainen viestintä arjen tekojen ohella ja lisäksi, ja niiden tueksi, ne ovat aivan keskiössä.

Tuija Kuusisto [00:24:17]: Kuinka sitten, jos on vielä hieman mietittävä tätä henkilökohtaista suhtautumistasi digitaaliseen turvallisuuteen. Kuinka Petri huomioit tämän digitaalisen turvallisuuden aivan omassa elämässäsi?

Petri Knape[00:24:34]: Totta kai huomioin, johtuen tuosta omasta ammattitaustastani. Pyrin parhaan kykyni mukaan huolehtimaan kaikista turvallisista toimintatavoista, jotka suinkin ovat mahdollisia. Mutta samaan aikaan viittaan siihen mitä totesin 100 prosenttisen turvallisuuden utopiasta. Yritän senkin ottaa arjessa huomioon. Niin että se turvallisuus ja sen ylläpitäminen eivät myöskään haittaa sitä arjen toimintaa. Vaan se haetaan se oikeanlainen tasapaino niissä asioissa, joiden kanssa ollaan tekemisissä, ja niihin liittyvässä suojaamistarpeessa. Ja hyväksyä kuitenkin johonkin rajaan asti se, että täydellistä suojaa digitaalisen turvallisuuden loukkauksille ei voi saavuttaa. Mutta että en omilla toimillani ainakaan sitä millään tavalla lisää. Tähän ehkä nostaisin, uskallan ATK-sukupolveen kuuluvana, liki 60-vuotiaana miehenä todeta, että tämä teknologinen kehitys on sellainen, että näillä ikävuosilla mukana pysyminen tässä voimakkaassa muutoksessa ja digitaalisen turvallisuuden ylläpitämisessä, ehkä konkreettisesti lisääntyvässä salasanojen maailmassa, niin asettaa kieltämättä haasteita. Ja pahimmassa tapauksessa ne nostavat mielestäni myös riskiä siitä, että jos turvajärjestelyt ovat käytännön arjessa liian vaikeita, niin ihmiset inhimillisistä syistä helposti saattavat jättää ne käyttämättä, tai sitten siirtyvät käyttämään sellaisia järjestelmiä, joita on helpompi käyttää, mutta joiden turvallisuus on huonompi. Ja tähän mielestäni pitäisi meidän digiarkkitehtuurissa, ja digitaalisten järjestelmien kehittämisessä, kiinnittää erityistä huomiota. Jotta se käyttäjäystävällisyys, ja arjen tarpeet

huomioitaisiin, ja tasapainoitettaisiin. Ja sitten niiden turvajärjestelyjen kanssa. Ja jokainen niissä oloissa pyrkisi maksimoimaan sen, että ei ainakaan omilla toimillaan lisää niitä turvallisuusriskejä.

Tuija Kuusisto [00:26:46]: Näinhän se on. Nopeasti opimme käyttämään maskejakin, kun kaikki havahduimme, että sitä tarvitaan. Ja turvavyökin muistetaan aina laittaa päälle kun mennään autolla liikkeelle. Pitää vain saada riittävän yksityiskohtaisesti, ja kuitenkin sillä selkeällä kielellä kerrottua, että mitä kannattaa tehdä, että oma digiturva on kunnossa. Uskon, että kaikilla kyllä siihen motivaatiota löytyy. Mutta kiitos paljon Petri, tästä [?? 00:27:19]. Ja oikein hyvää kesän alkua.

Petri Knape[00:27:24]: Sitä samaa teille, ja kiitos mukavasta keskustelusta. Ja Tuija tuo loppukommenttisi osui asian ytimeen. Kyllä me kaikki aikanaan opimme luultavasti, ja tahtotilaa siihen tulee löytyä.

Tuija Kuusisto [00:27:37]: Kiitos.

Kimmo Rousku [00:27:38]: Kiitos.

Petri Knape[00:27:39]: Kiitos.

[äänite päättyy]