Puolustusministeriö
Försvarsministeriet
Ministry of Defence

Lausunto

19.9.2022

VN/25733/2021
VN/25733/2021-PLM-219

Työ- ja elinkeinoministeriö

Puolustusministeriön lausunto Suomen digitaalisesta kompassista (2. luonnos)

Kansallinen digikompassi kokonaisuutena

Puolustusministeriö pitää hyvänä, että yhteiskuntaa katsotaan kokonaisuutena digitalisaatiokehityksen näkökulmasta. Yhteiskunnan keskeisten toimijoiden, eli viranomaistoimijoiden, elinkeinoelämän sekä järjestökentän mukaan ottaminen on kokonaisturvallisuuden mallin mukaista, ja siksi erityisen kannatettavaa. Kun kokonaisuutta rakennetaan yhdessä, digitalisaatioon saadaan toivottavasti olennaisena osana mukaan varautumisajattelu, jolloin tiekartan tulisi lähtökohtaisesti edistää digitalisaatiota turvallisuutta unohtamatta.

Puolustusministeriö kiinnittää kuitenkin huomiota siihen, että SWOT-analyysin uhissa todetaan vaatimattomasti, että ”Turvallisuus digitaalisissa ympäristöissä heikentyy ja haittaa yhteiskunnan toimintaa ja luottamusta viranomaisiin”. Käytännössä fyysinen maailma on saanut rinnalleen digitaalisen maailman. Nämä yhdessä muodostavat uudella tavalla toimivan kokonaisuuden. Pahimmillaan yhteiskunnan toiminta voidaan digitaalisesti lamauttaa, jolloin viranomaiset eivät kykene tarjoamaan peruspalveluita. Eri aikoina rakennettujen eri tasoisten ratkaisujen yhdistelmät voivat mahdollistaa tietoturva-aukkoja sekä sen, että järjestelmät eivät ole yhteensopivia. Järjestelmien hankinta ilman riittävää osaamista voi suoraan vaarantaa asioiden hoitamisen. Viranomaisten ja muiden toimijoiden digitaalisten palveluiden ulkoistaminen yksityisille yrityksille voi pahimmillaan aiheuttaa kriittisten palveluiden siirtymisen ulkopuolisen valtiollisen toimijan haltuun yritysjärjestelyiden ja yritysten ohjaamisen kautta.

Mahdollisuutena on hoitaa yllä mainitut asiat mallikelpoisesti, jolloin tavoitteet saavutetaan ja ylitetään ja tämän osalta voi syntyä myös laajaakin osaamisvientiä ja siten kansantalouden kasvua, mutta tämä vaatii selkeitä päätöksiä ja tarvittavat resurssit ml. rahoitus.

Kappaleessa Turvallisuus haastetaan uusilla tavoilla digitaalisessa ympäristössä (s. 12), kuvataan hyvin turvallisuuden merkitystä ja sitä, että se on otettava kaikessa huomioon. On tärkeää, että tämä viedään oikeasti käytäntöön, että ei käy niin, että turvallisuus jää vain kirjaukseksi sivulle 12 tai että toimista tehdään päälle liimattuja.

Kappaleessa Tiedon hyödyt kasvavat jakamalla (s. 8) todetaan, että ”Datatalouden, alustatalouden ja sujuvien digitaalisten palveluiden kehitys perustuu digitaalisen tiedon, eli datan sujuvalle jakamiselle eri toimijoiden välillä. Hyödyt syntyvät yhdistämällä ja analysoimalla dataa uusin tavoin esimerkiksi digitaalisten palveluiden pohjaksi. Ketterä ja reiluin ehdoin tapahtuva dataan pääsy kaikenkokoisille yrityksille sekä rohkeus avata dataa ja kehittää uudenlaisia liiketoimintamalleja luovat uutta datatalouden kasvuliiketoimintaa.” Tässä yhteydessä on tunnistettava yhteiskunnan toiminnan kannalta suojattava kriittinen tieto. Digitalisoituvassa maailmassa ylipäänsä on kriittistä huolehtia erilai-

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Puolustusministeriö PL 31 00131 Helsinki	Eteläinen Makasiinikatu 8 Helsinki	0295 16001 +358 295 16001		kirjaamo.plm@gov.fi www.defmin.fi

sista aineistoon ja sen käyttöön kohdistuvista riskeistä sekä kyberturvallisuudesta. Puolustusministeriö pyytää kiinnittämään huomiota siihen, että ennen laajojen tietoaineistojen digitalisointia ja avaamista on hyvä huolehtia riskiarviosta. Riskiarvion tekemisellä voidaan varmistua siitä, että alustojen tietoturvallisuus on riittävällä tasolla, että kasautumisvaikutusta ei pääse syntymään, ja että sensitiivinen tai kasautumisen kautta sensitiivinen data on tunnistettu ennakkoon. Näin voidaan hallita myös avattavien datavarantojen avulla tehtävää laaja-alaista vaikuttamista. Riskiarvio tulee tehdä ennen kuin tietovarantoja avataan tutkimus- ja kehityskäyttöön, ja sen aikana on erityisen tärkeää kuulla niitä tahoja, joiden tietoa sisältyy datavarantoon ja jonka avaaminen julkiseksi voi vaarantaa toimijoiden operatiiviset toimintaedellytykset. Valtiollisen näkökulman lisäksi tämä on tärkeää jalkauttaa osaksi alueellista riskiarviota, sekä tukea aktiivisesti yksityisen sektorin toimijoita sektorikohtaisten riskiarvioiden tekemiseksi. Lisäksi riskienhallintaa tulee tehdä jatkuvasti.

Puolustusministeriö esittää tuloksellisuuden seurannan osalta, että digikompassin toimenpiteiden edistymistä peilattaisiin myös kyberturvallisuusstrategiaan sekä yhteiskunnan turvallisuusstrategiaan niiltä osin, kuin se on olennaista.

Digitaalinen infrastruktuuri

Digitaalisen infrastruktuurin osalta paikkatiedon mukaan ottaminen on erittäin kannatettavaa. Tässä on kuitenkin huomioitava erityisen tarkkaan kriittisen infrastruktuurin ja yhteiskunnan elintärkeiden toimintojen paikkatieto sekä se, ettei niitä jaeta avoimesti kaikille. Erityisesti tarkkojen paikka- ja olosuhdetietojen osalta on tärkeää tehdä riskiarvio kriittiseksi katsottavasta tiedosta, ja suojata ja tehdä säännöllisesti päivittyvä riskienhallintasuunnitelma avattavien tietojen osalta proaktiivisesti ennen julkisen tiedon avaamista kehitys- ja innovaatiokäyttöön.

Digitaaliseen infrastruktuuriin olisi tärkeää laskea myös toimitusketjut, sekä pohtia miten keskinäisriippuvuus huomioidaan digikompassissa.

Yritysten digitalisaatio

On hyvä, että luonnoksessa on tunnistettu pk-yritysten digikehityksen esteitä, mutta konkretia jää hieman kaukaiseksi. Voisi pohtia millaisilla rakenteilla, esimerkiksi fasilitoiduilla, vertaisille järjestelyillä verkostoilla, voisi saada innostettua pk-yrityksiä digitalisoitumaan nopeammin.

Digitaaliset julkiset palvelut

Sivulla 41 todetaan kappaleessa Toimintaympäristön muuttuessa tavoitteena kokonaisturvalliset julkiset palvelut, että ”Kansalaisten, yritysten ja yhteisöjen tulee voida luottaa eettisesti kestäviin, avointa ja läpinäkyvää toimintaa tukeviin ja turvallisiin julkisiin palveluihin”. Erittäin hyvä kappale, mutta tärkeää tunnistaa se, että joissain tilanteessa avoimuuden ja läpinäkyvyyden vaatimus ei kättele turvallisuuden kanssa ja se on tärkeää hyväksyä.

Tietohallintojohtaja Mikko Soikkeli

Neuvotteleva virkamies Aulikki Pakanen

Liitteet

Jakelu TEM Työ- ja elinkeinoministeriö

Tiedoksi LVM TIO Tietoliiketoimintayksikkö, Merita Erkkilä
LVM TIO Tietoliiketoimintayksikkö, Maaria Mäntyniemi
VM JulkICT Tietopolitiikka, Anita Juho
OKM KTPO Korkeakoulupolitiikan vastuualue, Jonna Korhonen
TEM IYR YKTE Digitalisaatio-tiimi, Tiina Hanhike

VN/25733/2021-PLM-219

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Pakanen Aulikki 912189038	Soikkeli Mikko 91266073V
2022-09-19	2022-09-19