Puolustusministeriö
Försvarsministeriet
Ministry of Defence

Harri Mäntylä

13.9.2018

VN/3729/2018
VN/3729/2018-PLM-5

VM lausuntopyyntö VM/276/00.01.00.01/2018

Puolustushallinnon lausunto julkisen hallinnon linjauksiin tiedon sijainnista ja hallinnasta

Liitteenä puolustusvoimien ja puolustushallinnon rakennuslaitoksen lausunnot valtiovarainministeriön linjauksiin julkisen hallinnon tiedon sijainnista ja hallinnasta.

Puolustusministeriö toivoo lausuntojen huomioimista, vaikka määräaika lausuntojen antamiselle on jo mennyt.

Tietoturvapäällikkö Harri Mäntylä

Liitteet Puolustusvoimien lausunto
Puolustushallinnon rakennuslaitoksen lausunto

Jakelu VM Valtiovarainministeriö

Tiedoksi VM Valtiovarainministeriö, Pauli Kartano

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi

Puolustusministeriö

PL 31
00131 HELSINKI

Puolustusministeriön lausuntopyyntö AO13780/ 24.7.2018

LAUSUNTO JULKISEN HALLINNON LINJAUKSESTA TIEDON SIJAINNISTA JA HALLINNASTA

Puolustusministeriö on pyytänyt Pääesikunnan lausuntoa Valtiovarainministeriön luonnoksesta ”Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta”.

Tämän lausunnon taustalla vaikuttavat Puolustusvoimissa valmisteilla oleva TUVE strategia ja pilvipalvelustrategia, jotka määrittävät Puolustusvoimien palvelutuotannon tavoitteet lähivuosina.

Lausuntopyynnön kohteessa olevassa valmistelussa tulisi tarkentaa, onko kyseessä hallinnollisesta määräyksestä, ohjeesta tai pelkästään suosituksesta (634/2010, tietohallintolaki 4§).

1 Lausunnon perustelut

Pääesikunta on arvioinut julkisen hallinnon tietohallinnon ohjauksesta annetun lain (634/2010, tietohallintolaki) 4 §:n mukaista *tietohallinnon ohjauskysymystä* mm. pilvipalveluihin liittyvien linjausten osalta.

Tietohallintolain 2 § 2 momentin soveltamisalaa koskevassa säännöksessä todetaan, että *viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) tarkoitetusta valtion viranomaisen tietoturvasta ja valmiuslaissa (1080/1991) tarkoitetusta valtion viranomaisen poikkeusoloihin varautumisesta on tietohallinnossa voimassa, mitä niistä säädetään mainituissa laeissa*.

Voimassa olevan valmiuslain (1552/2011) 105 §:ssä todetaan edelleen, että *valtiovarainministeriö voi määrätä poikkeusoloissa valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tieto-*

turvallisuuden järjestämisestä (1 mom.); ja että, ***valtiovarainministeriön ohjaus ei koske kuitenkaan Puolustusvoimien, rajavartiolaitoksen, poliisin, pelastus-viranomaisten ja hätäkeskusten toiminnallisia tieto-järjestelmiä*** (2 mom.).

Hallituksen esityksessä valmiuslaiksi (HE 3/2008 vp., 105.2 §, yksityiskohtaiset perustelut) *rajataan ohjauksen ulkopuolelle Puolustusvoimien, rajavartiolaitoksen, poliisin, pelastus-viranomaisten ja hätäkeskusten* ***toiminnalliset tietojärjestelmät****,* ***jotka ovat välttämättömiä poikkeusoloissa****. Tällaisia järjestelmiä olisivat esimerkiksi Puolustusvoimien tiedustelu- ja valvontajärjestelmät, rajavartiolaitoksen johtamisjärjestelmä ja hätäkeskuksen tietojärjestelmä*.

Pääesikunta on katsonut tämän perusteella Puolustusvoimien käytössä olevan toiminta-, tieto-, järjestelmä- ja teknologia-arkkitehtuurin painottuvan pääosin valmiuslain 105 §:ssä tarkoitettuihin toiminnallisiin tietojärjestelmiin, jotka ovat välttämättömiä poikkeusoloissa. Toisaalta tilanne ei ole selkiytynyt kaikilta osin mm. *«julkisen» «hallinnon» tietohallinnon yhteisten palvelujen ja muiden tietohallintoon liittyvien yhtenäisen toiminnan kannalta tarpeellisten toimenpiteiden ja tietojärjestelmien osalta*.

Toistaiseksi on huomioitava edelleen se, että pääosa Puolustusvoimien käytössä olevista tietojärjestelmistä on määritelty ja toteutettu siten, että järjestelmien toiminnallinen, tiedonohjaussuunnitelmaan perustuva, luokitus käsittää erilaisia hallinnon toimintamuotoja. Järjestelmäkohtaisessa tarkastelussa on huomioitava esim. se, että asejärjestelmähankkeiden ja hankintaprosessin valmistelussa tapahtuu hallintolaissa tarkoitetun ***hallintoasian*** valmistelun lisäksi myös asejärjestelmien teknistä vaatimusmäärittelyä ja elinjakson hallintaan liittyvää dokumentointia. Käytössä oleviin asejärjestelmiin liittyvää valmistelua tulisi siten arvioida myös ***sotilaskäskyasioina*** ja valmistelu on tavallisesti yhteydessä *operatiiviseen ja strategiseen suunnitteluun*. Puolustusvoimien toiminnallisissa järjestelmissä on siten korostettava *tieto-turvallisuuden* ja erityisesti *kansainvälisten tietoturvavelvoitteiden* huomioimista ***maanpuolustuksen edun*** lähtökohdista.

Turvallisuusviranomaisten poikkeavasta näkökulmasta johtuen olisi mahdollisesti hyvä tarkentaa tietohallintolakiin perustuvaa valtiovarainministeriön ja samalla myös muiden ministeriöiden tehtävän *ohjata toimialansa tietohallinnon ja tietohallintohankkeiden kehittämistä ottaen huomioon tässä laissa säädetyt tarkoitukset ja velvoitteet* merkitystä mm. siinä suhteessa missä määrin ko. linjausten yhteydessä on kysymys *hallinnollisesta määräyksestä* tai *ohjeesta* tai sitten vain korostamalla linjausten merkitystä *suosituksena,* johon valmiuslaissa tarkoitetut turvallisuusviranomaiset voivat halutessaan tukeutua.

2 Linjausten arviointi

2.1 Tietoturva- ja kyberturvallisuus

Mikäli pilvipalveluihin tukeutumista halutaan arvioida turvallisuusviranomaisten ja erityisesti puolustusvoimien tietohallinnossa, tulisi asiaa tarkastella kansainvälisistä tietoturvallisuus-velvoitteista annetun lain (588/2004) 3 §:ssä tarkoitettujen kansainvälisten tietoturvavelvoitteiden tasalta kotimaisen tai toisen valtion, kansainvälisen järjestön ja siellä kotipaikkaansa pitävän yrityksen sekä tässä yhteydessä tarkoitettujen valtiosopimusten ja turvallisuusluokiteltujen sopimusten lähtökohdista. Tässä merkityksessä linjaus Suomeen, Euroopan Unioniin tai ETA-alueeseen ja muihin maihin on riittämätön. Lisäksi EU tietosuoja-asetuksen velvoitteet henkilötiedon sijainnista tulee ottaa huomioon.

Pilvipalveluihin tukeutuminen ei ole perusteltavissa tietoturvallisuuden etuna edes suojaustasoa ST IV olevan tiedon yhteydessä. Riskinä nähdään, että näiden linjausten perusteella ratkaisuja tehdään joko tai ei vaihtoehtoihin perustuen tai ilman asian edellyttämää tapauskohtaista oikeudellista tulkintaa. Suojaustason ST IV ja jopa julkisen tiedon yhteydessä on huomioitava kasautumisvaikutus sekä toisaalta myös järjestelmien käyttövaltuushallinnan rekisterinpidosta johtuen tarve suojata yksityisen edun lisäksi myös julkista etua (operatiivisesti merkittävät erityisryhmät).

Tiedon ja palveluiden sijainnin yhteydessä tulisi huomioida laajemmin kansainvälisten tietoturvavelvoitteiden merkitystä.

2.2 Palvelutuotanto

2.2.1 Linjaukset

Linjaus 1: Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta.

Linjaus on tarkoituksenmukainen. Puolustusvoimat turvallisuusviranomaisena on velvoitettu käyttämään TUVE lain mukaisia TUVE- palveluita. Kokonaisharkinta palvelujen hankinnasta ja käytöstä tehdään sotilaallisen maanpuolustuksen lähtökohdista.

Linjaus 2: Tiedon sijaitessa Suomen rajojen ulkopuolella erityistä on kiinnitettävä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen.

Tiedon käyttämisen, hallinnan sekä valvonnan mahdollistamiseksi Suomen rajojen ulkopuolella tulee ottaa huomi-

oon tarvittavien, kansainvälisessä käytössä, hyväksyttyjen suojausratkaisuiden käyttö sekä integrointi.

Palveluiden sijaitessa pilvimalleissa ulkomailla tai kolmannen osapuolen hallussa reaaliaikainen kyber- ja tietoturvatilannekuva on pakollinen vaatimus. Tämän lisäksi palvelun sopimusten laatimisessa tulee huomioida tietoturvapoikkeamien käsittely.

Linjaus 3: Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset.

Linjaus on tarkoituksenmukainen.

Linjaus 4: Mikäli pilvipalvelut tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita.

Tämä linjaus tulisi olla kolmannen linjauksen alakohtana.

Linjaus 5: Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti vähintään kerran vuodessa ja oleellisten sopimusehtojen muuttuessa.

Palvelun hyödyn arviointi on aina palvelun asiakkaan vastuulla. Yhteiseen palveluhankintaan liittyen yhteinen kriteeristö arvioinnille on välttämätön. Sotilaallisen maanpuolustuksen näkökulmasta palveluhyödyn ja -takuun muutos on riittävä peruste palvelun käytön lopettamiselle.

Linjaus 6: Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista.

Mitä tässä tarkoitetaan viranomaisella? Miten todetaan hyväksytyt palveluntarjoajat ja miten hyväksytyksi palvelutarjoajaksi pääsee? Tämä on keskeinen linjaus ja tulee määritellä tarkasti.

Linjaus 7: Julkisen tiedon käsittelyä ei rajoiteta

Tämä linjaus ei ole yksiselitteinen. Myös julkisen tiedon käsittelyssä tulee tiedon omistajan arvioida tiedon kasautumisvaikutusta. Tällä voi olla merkittävä vaikutus palvelumallin valintaan.

Linjaus 8: Henkilötietoa ja suojaustason IV tietoa voi käsitellä julkisessa pilvessä, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu

Tämä linjaus on tarkoituksenmukainen.

Linjaus 9: Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

Liittyy linjaukseen kuusi. Viranomaisen hyväksynnän perustana on oltava selkeä ja yhdenmukainen kriteeristö. Tämän lisäksi on määriteltävä prosessit joilla arvioinnit toteutetaan sekä arvioinnin toteuttamiseen oikeutetut tahot.

2.2.2 Palvelumallit

Kappaleessa 4.2. on kuvattu palvelumallit. Puolustusvoimien käsityksen mukaan palvelumallien yhtenäinen kuvaaminen läpi valtionhallinnon on lähtökohta sille, että pilvipalvelut käsitetään samalla tavalla.

Eri palvelumallien hankkimiselle tulisi olla erilliset kriteeristöt. Esimerkiksi SaaS -palvelun hankkiminen on kaikista monipuolisin yhdistelmä eri toimijoita, jolloin alusta-, sovellus-, middleware- palvelut saattavat tulla eri toimijoilta. Usean toimittajan ketju on riski turvallisuudelle, koska pilvipalveluiden kokonaisturvallisuuden määrittää sen heikoin lenkki.

2.2.3 Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Sivulla 9 on kuvattu riskienhallintaa tiedon sijainnin ja luottamuksellisuuden suhteen. Toiminnan jatkuvuus poikkeusoloissa saattaa olla joissain tilanteissa paremmin turvattuna, jos palvelu on yksityisen hallussa. Yksityinen muu - termi kaipaisi lisämäärittelyä.

Sotilaallisen maanpuolustuksen kannalta poikkeus- ja häiriöoloissa (ennen valmiuslain voimaantuloa) tulee erikseen määritetyt pilvipalvelut olla turvattuna ja palautettavissa sekä jatkuvuussuunnittelu olla tehtynä. Nämä asiat huomioidaan sopimuksissa, joihin liittyy viranomaissuunnittelua ja vaatii yritykseltä syvempää kumppanoitumista. Kansainvälinen lainsäädäntö tulee ottaa huomioon, kun palvelua viedään rajojen ulkopuolelle.

3 Suosituksia jatkotoimenpiteiksi

Yleisesti voidaan todeta, että esitetyt jatkotoimenpiteet ovat relevantteja. Toimijoiden vastuujakoa linjausten toimeenpanossa on kuitenkin selvennettävä. Sotilaallisen maanpuolustuksen näkökulmasta kyber- ja tietoturvallisuustilannekuvan muodostaminen ja ylläpito tulee lisätä vastuunjakotaulukkoon.

Turvallisuusviranomaisten palveluiden ja hallinta tulee linjauksissa olla tarkemmin määritelty varsinkin tilanteissa, jolloin tieto tai palvelu, tai näiden hallinta tapahtuu Suomen ulkopuolelta.

Vaatimus palvelutuottajien turvallisuusselvityksistä tulee jatkossa ottaa huomioon.

Auditointi tulee olla yhteismitallinen ja velvoittava eri palvelutuotantomalleissa. Auditointikriteeristöön tulee liittää riskienhallinnan mittaristo, jonka pohjalta voidaan määrittää hyväksyttävä jäännösriski.

4 Johtopäätökset

Linjaukset ovat relevantteja ja antavat mahdollisuuksia oman toiminnan kehittämiseksi. Turvallisuusviranomaisille on annettava mahdollisuus toteuttaa omien lakisääteisten tehtävien toteuttaminen omien lähtökohtien ja tarpeiden mukaisesti. Tämä on keskeinen vaatimus sotilaallisen maanpuolustuksen kannalta. Näiden linjausten poikkeamien käsittelyyn tulee laatia prosessit ja niitä käsittelevät elimet, mikä on erityisen tärkeää tarkasteltaessa turvallisuusviranomaisten yhteisten palveluiden tuottamista pilvipalveluna.

VM:n tulee huolehtia siitä, että linjausten toimeenpanon liittyvät prosessit ja toimintatavat tukevat linjausten tavoitteiden saavuttamista.

Turvallisuusviranomaisille tulee mahdollistaa häiriö- ja poikkeusoloissa oman toiminnan kannalta kriittisten palveluiden kapasiteetin siirto omiin laitetiloihin ja toiminnan jatkuvuuden turvaaminen.

Eri pääpalvelumallien konkretisointi ja niiden erilaiset turvallisuuspainotusten huomioon ottaminen vaatii lisätarkastelua. Esimerkiksi SaaS palveluiden käyttö- ja tietoturvallisuusvaatimukset poikkeavat merkittävästi muista palvelumalleista.

Allekirjoitukset

Allekirjoitusteksti

LIITTEET

JAKELU

TIEDOKSI

VN/3729/2018, VN/3729/2018-PLM-3

PUOLUSTUSHALLINNON RAKENNUSLAITOKSEN LAUSUNTO VALTIOVARAINMINISTERIÖN LUONNOKSESTA "JULKISEN HALLINNON LINJAUKSET TIEDON SIJAINNISTA JA HALLINNASTA"

Viitekohdassa mainitun asiakirjan johdosta Puolustushallinnon rakennuslaitos ilmoittaa lausuntonaan seuraavaa:

Yhteenveto

Rakennuslaitos toteaa, että olisi hyvä, jos julkisen hallinnon tiedon sijaintia ja hallintaa määrittäisivät yhteiset ja yhteisesti noudatettavat periaatteet, kuten asiakirjan tavoitteeksi on asetettu. Samalla Rakennuslaitos korostaa, että pilvipalveluihin ja niiden käyttöönottoon liittyy problematiikkaa, johon on hyvä saada reunaehdot erityisesti puolustushallintoa ja turvallisuusviranomaisia koskien.

Lausunnolla olevassa linjausluonnoksessa on vielä ristiriitaisuuksia ja epäselvyyksiä. Esimerkiksi valmisteilla oleva Tiedonhallintalaki ja tässä asiakirjassakin mainitut muutokset kyseenalaistavat linjauksia ja jättävät linjausten toimeenpanoaikataulun epäselväksi.

Taustaa linjauksille

Kohtaan ei ole lausuttavaa.

Linjausten tavoitteet

Turvallisuusviranomaisten erityistarpeiden tulisi näkyä myös linjausten tavoitteissa.

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

4.1. Pilviteknologian edut

Pilvipalveluteknologian etuja (kuva 1) listattaessa kustannustehokkuus

nousee esille liian korostetusti. Turvallisuusviranomaisen näkökulmasta tietoturva on vähintään yhtä tärkeää.

Linjausten mukaisesti pilvipalveluiden käyttöönotto vähentää organisaatioiden oman osaamisen tarvetta. Puolustushallinnon rakennuslaitoksen toiminnan luonteen vuoksi palvelun käyttöönottoon, ylläpitoon ja sen tietoturvallisuuteen liittyvää osaamista ei ole mahdollista kokonaan ulkoistaa palveluntuottajalle.

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Palveluiden sijainnin, hallinnan ja ohjauksen riskit (kuva 2) nousevat Puolustushallinnon rakennuslaitoksen näkemyksen mukaan suuriksi (kuvan punainen väri) jo tiedon sijainnin ja/tai hallinnan ollessa EU-alueella. Yksityinen pilvipalvelu Suomessa aiheuttaa kuvan mukaisen keskitason riskin (kuvan oranssi väri).

Kuvassa 3 (Tiedon luottamuksellisuuden ja toiminnan jatkuvuuteen erityisesti poikkeusoloissa liittyvät riskit suhteessa palveluntuottamiseen liittyvään malliin) tavoiteltu tietosisältö jää erittäin epäselväksi.

Linjauksessa organisaatiolle vastuutetaan velvollisuus arvioida tiedon ja palvelun kriittisyyteen, tärkeyteen ja jatkuvuuteen liittyvät tekijät. Nykyisen toimintamallin mukaisesti, jossa virastoille tarjotaan valtion yhteisiä palveluita palveluntuottajan hankkimana (TORI-palvelut) yksittäisellä virastolla ei ole mahdollisuutta toimia linjauksen edellyttämällä tavalla.

5.1.2 Tietojen luokittelu

On hyvä, että linjaukset tietojen luokitteluun on annettu. Turvallisuusviranomaisten salassa pidettävää tietoa sisältävään palveluun liittyvässä riskienarvioinnissa tulee tiedon luonteesta johtuen erityisesti huomioida kasaantumisen aiheuttama suojaustason mahdollinen nousu jo ST IV alkaen.

5.3. Haasteet

Kappaleen alussa on hyvin tunnistettu pilvipalveluiden haasteita. Kappaleen sisältö ja sen tarkoitus jää kokonaisuudessaan kuitenkin epäselväksi. Esimerkiksi se, että valtiovarainministeriössä tehtävä Tiedonhallintalain valmistelu tulee muuttamaan tietojen luokittelua, tekee asiakirjassa esitellyt linjaukset epävarmoiksi.

Linjaukset julkisen hallinnon tiedon sijainnista ja hallinnasta

Linjauksiin julkisen hallinnon tiedon sijainnista ja hallinnasta toivotaan tarkennuksia.

Linjauksessa 6 jää epäselväksi, mikä viranomainen jatkossa ylläpitäisi listaa hyväksytyistä palveluntarjoajista.

Linjaukseen 8 olisi toivottavaa saada tieto siitä, mitä on asianmukainen toteuttaminen ja todentaminen.

Linjaus 9: Mikä viranomainen hyväksyy ST III –pilvipalvelut?

Linjaus 9: ”*Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa. Tällaisen tiedon käsittelyyn käytettävän pilvipalvelun täytyy sijaita fyysisesti Suomessa tai EU:n alueella…”* on ristiriidassa kappaleen 5.1.2 Tietojen luokittelu kanssa, jonka mukaan ”*ST III tai turvallisuusluokiteltavaa ST III LUOTTAMUKSELLINEN tai korkeampi tietoa, tietoa saa käsitellä ainoastaan Suomessa ja omassa hallinnassa olevia palveluita hyödyntäen*”.

Linjausluonnoksessa ehdotetut jatkotyöt toteutettuina (arviointipankki, pilviohje, yhteisten sopimusehtojen riskianalyysipohja ja pilviarkkitehtuuri) auttavat yksittäisten viranomaisten toimintaa.

Ritva Peura
Hallintojohtaja

Anu Hakkarainen-Kiri
Tietoasiantuntija

Tämä asiakirja on sähköisesti allekirjoitettu

JAKELU Puolustusministeriö