EDUSKUNNAN APULAISOIKEUSASIAMIES

Helsinki 1.10.2013 Dnro 4071/5/13

Valtiovarainministeriö
Julkisen hallinnon ICT-toiminto
PL 28
00023 Valtioneuvosto

Viite: Kirjeenne 17.9.2013

LAUSUNTO

Valtiovarainministeriö on viitekohdassa mainitussa kirjeessään pyytänyt muiden ohella eduskunnan oikeusasiamieheltä lausuntoa VAHTI-ohjauksessa valmistellusta Päätelaitteiden tietoturvallisuusohjeesta ja siihen liittyvistä tukimateriaaleista. Tähän liittyvät kolme 1.10.2010 voimaan tulleen tietoturvallisuusasetuksen (681/2010) täytäntöönpanon yhteydessä annetut VAHTI-ohjeet 2/2010, 3/2010, 3/2012 sekä 2/2012.

Lausuntonani esitän kohteliaimmin seuraavan.

1
JULKISEN HALLINNON TIETOTURVALLISUUDEN NYKYTILASTA

Aikanaan valtionhallinnon käyttämien päätelaitteiden hankinta oli hyvinkin valtiovarainministeriön silloisen järjestelyosaston keskitetyssä ohjauksessa (vrt. asetus automaattisesta tietojenkäsittelystä valtionhallinnossa 212/1975, sittemmin 188/1988 ja 756/2003). Nykyisin päätelaitteiden kirjo ja tietohallintoyhteistyön tarve ovat moninkertaistuneet.

Tietoturvallisuus verkottuvassa hallinnossa on monesta eri syystä erittäin ajankohtainen asia. Tietoturvallisuus on monivuotisen VAHTI-työn jälkeen yhdenmukaistumassa (vrt. myös EOA:n lausunnot valtiovarainministeriölle 21.10.2010 dnro 3404/5/10; sosiaalinen media ja sisäasiainministeriölle 28.4.2011 dnro 1339/5/11; identiteettiohjelma).

Ohjeluonnoksessa keskitytään viranomaistoiminnan tietoturvan erityiskysymykseen eli turvaluokiteltujen sisältöjen käyttöön ja eri päätelaitteiden käytön tuomaan tietoturvariskiin. Silti on syytä muistaa, että turvallista hallintoa ja kansalaisten asiointia toteutetaan ja ylläpidetään organisaatioissa tietoturvallisuuden kokonaishallinnan avulla (ks.

Osoite: 00102 Eduskunta
Puhelin: (09) 4321
Telefax: (09) 432 2268
Sähköposti: oikeusasiamies@eduskunta.fi
Internet: www.oikeusasiamies.fi

myös www.tietohallintomalli.fi). Tietojohtamisessa hallintajärjestelmä toteuttaa organisaation strategiaa ja kattaa tietoturvallisuuden 1) yksityiskohtaisen organisoinnin 2) henkilöstön tehtäväkuvat 3) toimintapolitiikat, suunnittelun ja vastuut 4) menettelytavat ja prosessit sekä 5) tarvittavat resurssit.

Päätelaitteiden haavoittuvuuksien hyväksikäyttö, hyökkäykset ja rikollinen toiminta muuttuu kokoajan entistä kehittyneempään, jopa automatisoituun suuntaan. Tämä on vaikuttanut palveluiden heikentymiseen, tiedon katoamiseen ja pahimmassa tapauksessa viraston tai yrityksen maineen menetykseen. Tietoturva-auditoinneissakin on havaittu monikäyttöisten päätelaitteiden, kuten tablettitietokoneiden, tuoneen uudenlaisia haasteita tietoturvalle. Ongelmana tietosisältöjen salassa pidossa voi myös olla Linux-käyttöjärjestelmän asentaminen samaan päätelaitteeseen ja alun perin Windows-toimintaympäristöön.

Näitä turvallisuusasioita julkishallinnon organisaatio ei voi hoitaa yksin vaan monet yksityisten kansalaisten ja organisaatioiden verkkoyhteydet kytkeytyvät asiointi- ja palveluverkoissa viranomaisverkkojen rajapintoihin. Myös VAHTI-ohjeissa korostetaan, että tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi.

Päätelaiteohjeen tarkoituksena on tukea valtionhallinnon toimijoita päätelaitteilla tai niiden välityksellä tapahtuvan tietojen käsittelyn turvaamiseksi. Yhtä hyvin eri päätelaiteriskeistä ja verkkoasioinnin mahdollisuuksista (mobiilivarmenteet) kertominen olisi tärkeätä hallinnon asiakkaiden kannalta. Nyt arvioitava ohje on sinänsä johdonmukainen kehitysaskel VAHTI-ohjeiden ajantasaistamiseksi, mutta yleinen kehys on hankeryhmän kokoonpanonkin huomioon ottaen varsin tietotekninen ja koulutuksellinen.

Samalla julkinen hallinto on sitoutunut Avoimen hallinnon kumppanuusohjelmassa kansainvälisestikin kehittämään hallintotoimintojen läpinäkyvyyttä (ks. http://www.vm.fi/vm/fi/05_hankkeet/0238_ogp/-index.jsp). Samoin on lupauduttu parantamaan asiakirjojen ja tallenteiden saatavuutta (Euroopan neuvoston konventio pääsystä virallisiin asiakirjoihin 205/2009: oikeusministeriö valmistelee; http://conventions.coe.int/Treaty/en/Treaties/Html/205.htm). Päätelaiteohjeessa korostetaan useassa kohdin salassapidon toteuttamista mutta yhtä tärkeitä nykyaikaisessa hallinnossa ovat verovaroin kerättyjen julkisten tietojen saatavuus ja avoimen datan käyttömahdollisuudet.

Laillisuusvalvonnan näkökulmasta totean, että tietoturvallisuudesta, arkaluonteisten henkilötietojen käsittelystä ja asiakastiedoista on säädetty useassa eri laeissa.

Siten viittaankin lausuntooni valtiovarainministeriölle 10.10.2011 (DNro 3415/5/11, s. 3). Lausunto koski VAHTI-ohjauksessa valmisteltua Johtajan tietoturvallisuusoppaan luonnosta. Nyt olisi pantava uu-

delleen merkille se, että tietoturvallisuus on osa perustuslain (731/1999) 21 §:n tarkoittamaa hyvää hallintoa. Tietoturvallisuudella suojataan lainmukaisuuden saavuttamiseksi organisaation omaan toimintaan, yhteiskunnan toimintaan sekä kansalaisiin liittyviä tietoja.

Tähdennän uudelleen, että lainmukaisuuteen (ohjeen suppea luettelo s. 9) olisi perusteltua lisätä siinä mainittujen lakien lisäksi viittaukset perustuslakiin, hallintolakiin sekä varsinkin lakiin sähköisestä asioinnista viranomaistoiminnassa (erit. 5 § 3 momentti). Lain velvoituksin viranomaisen on pyrittävä käyttämään *asiakkaan kannalta teknisesti mahdollisimman yhteensopivia ja helppokäyttöisiä laitteistoja ja ohjelmistoja.* Viranomaisen on lisäksi varmistettava riittävä tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa.

2 PÄÄTELAITEIDEN MONINAISUUS

Käytännössä viranomaiset omissa tietoverkoissaan ja hallinnon asiakkaat ottavat yhteyttä viranomaisiin yhä useammin mobiililaitteilla, joiden käyttöjärjestelmät ja selainohjelmistot ovat moninaisia. Tähän heitä myös monin paikoin palveluverkoissa kannustetaan. Olennaisia asioita tulevaisuuden tietoteknisessä toimintaympäristössä tulevat olemaan hallinnon fyysisten toimipisteiden väheneminen, toimintojen virtualisointi, virastojen etätyön lisääntyminen sekä yksityisten organisaatioiden ja korporaatioiden lisääntyvä rooli. Päätelaiteohjeessa on enimmillään puhuttu yhteistyökumppaneista (s. 4) mutta ei demokraattisesti verkkopalveluita käyttävistä kansalaisista tai kansalaisliikkeistä.

Päätelaiteohjeessa (jakso 3, s. 12 ss.) on tietoturvallisuuden näkökulmasta arvoitu tyypillisiä uhkia ja huomioitavia asioita. Oppaan sisältöä olisi voitu tältä osin selkeyttää ajantasaisella päätelaitteiden valikoiman kuvauksella päätelaite terminä tulisi määritellä ja listata yhteen paikkaan listaus valikoimasta. Nyt päätelaitteita luetellaan ohjeessa siellä täällä ilman yhtenäistä logiikkaa. Myös päätelaitteiden käyttötilanteet, esim. ulkomaisessa lähialueiden poliisiyhteistyössä, saattavat tuoda omat haasteensa tietoturvallisuuden säilyttämiselle.

Sosiaalista mediaa voidaan mahdollisesti käyttää myös viranomaisten hallinnassa olevilla päätelaitteilla ja tämäntyyppiseen käyttöön liittyvää tietoturvariskiä on todellakin aiheellista korostaa. Varsinkin eri tietoteknisten komponenttien ja sosiaalisen median palveluiden käyttö olisi voitu ottaa mukaan päätelaitteiden tietoturvallisuuteen. Päätelaitetunnistuksen ja selaintunnistuksenkin osalta asiaa olisi voitu ohjeen puitteissa syventää (vrt. http://fi.wikipedia.org/wiki/-P%C3%A4%C3%A4telaitetunnistus).

3 PÄÄTELAITEOHJEEN RAKENNE JA SISÄLTÖ

Päätelaitteelle on ohjeessa (s. 9) annettu laajasti mutta organisaatiokeskeisesti määritelmäksi "laite, jolla loppukäyttäjät ja pääkäyttäjät käyttävät organisaation tietoja sähköisissä tietojärjestelmissä tai muissa palveluissa".

Yleisemmin päätelaite (lyh: DTE, Data Terminal Equipment, usein myös terminaali) on tietoliikenneyhteyden päässä oleva laite, jonka avulla varsinainen kommunikointi tapahtuu tietoliikenneyhteyden kautta. Päätelaitteilla on kaksi tehtävää: 1) muuntaa käyttäjän tieto tietoliikenneyhteyden läpi välitettäviksi signaaleiksi ja 2) toimia verkkoon dataa lähettävänä asemana, joka välittää signaalia linkkiprotokollan mukaan. Päätelaitteita ovat esimerkiksi puhelimet (puhelinverkon päätelaite), matkapuhelimet (GSM-verkon päätelaite) tai tietokoneet (esimerkiksi Ethernet-verkon päätelaite tai tieliikenteen valvontalaite). Verkkopalvelu mukautuu yleensä käyttäjän päätelaitteelle, eikä se edellytä käyttäjän mukautuvan palvelun tekniseen toimintaympäristöön.

Ohjeessa (s. 18) käsitellään eräänä näkökulmana salaamattoman sähköpostin käyttöä salassa pidettävien tietojen välittämiseen. Tältä osin oikeusasiamiehen puolelta on useissa päätöksissä katsottu, ettei salassa pidettäviä tietoja saa lähettää suojaamattomassa sähköpostissa (EOA Jääskeläisen päätös dnro 3438/4/09/24.3.2011 ja päätökseni dnro 2664/4/12/2.5.2013). Myös tietosuojavaltuutettu on sivunnut kannanotoissaan sähköpostin ja tekstiviestien ja siten päätelaitteiden käyttöä terveydenhuollossa (ks. (Tietosuojavaltuutetun kannanotto 1.7.2010; Dnro 1475/41/2009). Näitä hyvään hallintoon ja tiedonhallintotapaan ohjaavia ratkaisuja ei ole otettu huomioon päätelaiteohjeen luonnoksessa (vrt. myös https://www.turvaposti.fi/index.php?act=why).

Sivulla 14 viitataan päätelaitteen katoamiseen tai varastamiseen liittyviin tietoturvaohjeisiin. Samaa asiaa käsitellään myös sivuilla 25, 26 ja 31. Kuitenkin näyttää siltä, että ohjeistusta voitaisiin täsmentää. Ainoastaan sivulla 36, luvussa 8.4., ensimmäisessä esimerkissä kerrotaan konkreettinen esimerkki siitä, miten tätä tietoturvaa voidaan parantaa hankkimalla mobiililaitteiden hallintaohjelmisto (MDM – Mobile Device Management).

Pyydän harkitsemaan, voitaisiinko sivulta 32 alkavaan päätelaitepolitiikkaa ja ohjeistusta kuvaavaa taulukkoa täydentää. Ensiksi kadonneen päätelaitteen tietosisältöjen tyhjentäminen olisi perusteltua tehdä luotettavalla, keskitetyllä hallintaohjelmistolla. Toiseksi kadonnut päätelaite olisi voitava poistaa verkossa sallittujen laitteiden listalta, jolloin laitteen avulla ei enää päästä käsiksi mihinkään viranomaisen hallussa oleviin järjestelmiin eikä sisältöihin.

Lopuksi sinänsä selkeän oppaan kieltä ja kieliasua voitaneen vieläkin tarkistaa ja pyrkiä tietoturvallisuuden ammattiterminologiasta selkokielisyyteen. Pienehköt kirjoitusvirheet ja paikoin outo terminologia (kuten päätelaitteiden terveystarkastukset: olisiko kuntotarkastus) olisi perusteltua niin ikään korjata.

Hyvän hallinnon takeiden kannalta katson, että myös hallinnon asiakkaita tulisi muistaa ja laatia heidän käyttöönsä oma päätelaiteohjeensa (vrt. jo http://www.laatuaverkkoon.fi, kohta 1.3 ja Tietosuoja-lehti 3/2013 s. 26-29 sekä http://www.oikeus.fi/57282.htm).

Apulaisoikeusasiamies Jussi Pajuoja

Esittelijäneuvos Jorma Kuopus