YLIOPISTOJEN SEC-RYHMÄ LAUSUNTO 14.2.2006

Valtiovarainministeriö
Kirjaamo
PL 28
00023 VALTIONEUVOSTO

Viite: VM101:00/2005

ASIA: LAUSUNTO VALTIONHALLINNON IT-STRATEGIASTA

Suomalaisten yliopistojen tietoturvayhdyshenkilöiden yhteistyöverkostona toimiva Sec-ryhmä ilmaisee tukensa valtion tietojärjestelmien ja niihin liittyvän toiminnan yhdenmukaistamiseen suuntaavalle toiminnalle. On tärkeää, että päällekkäisen työn ja päällekkäisten toimintojen määrää valtionhallinnossa tarkastellaan kriittisesti. Ryhmä pitää positiivisena signaalina tietoturvallisuuden huomioimista ja erityisesti sitä, että tietoturvan rooli jo tietojärjestelmien hankinnan esitutkintavaiheessa on strategiassa tunnustettu.

Sec-ryhmä pyrkii esittämään tässä lausunnossaan yliopistomaailmaa laajemman tietoturvallisuuteen painottuvan näkökulman.

Peruspalveluiden tuottaminen

Yhteiset tai yhtenäiset järjestelmät ovat sinänsä kannatettavia, mutta yhteisyyden taso kaipaa tarkennusta. IT-komponenttien vakiointi ja yhteiset rajapintamäärittelyt ovat jo sellaisenaan merkittävä etu, jolla on laajoja positiivisia kustannusvaikutuksia. Usean samanlaisen järjestelmän sulauttaminen yhdeksi keskitetyksi järjestelmäksi ei välttämättä enää tämän jälkeen tuo merkittäviä lisäetuja.

Kaikkien IT-palvelujen keskittäminen myös laitetasolla palvelukeskuksiin kasvattaa merkittävästi virastojen tärkeiden prosessien käytettävyyteen liittyviä riskejä. Esimerkiksi sähköposti on muotoutunut yhdeksi tärkeimmistä viestintävälineistä. Viraston ja palvelukeskuksen välinen tietoliikenneongelma aiheuttaisi täten laajavaikutteisen häiriön viraston viestintäprosessissa.

Sähköpostin palvelujärjestelmän siirtäminen virastosta palvelukeskukseen voi sisältää vähemmän hyötyjä ja enemmän haittoja kuin on arvioitu. Selvää on, ettei kaikilla virastoilla ole resursseja huolehtia omasta sähköpostijärjestelmästä itse. Sellaisenaan tämä ei vielä tarkoita järjestelmän siirtopakkoa palvelukeskukseen. Valtion sähköpostin konsepti on joka tapauksessa viisasta vakioida, jolloin palvelujärjestelmä näyttäisi samanlaiselta virastosta riippumatta. Järjestelmän fyysinen sijainti voi olla viraston tiloissa, mikäli viraston tilat sen sallivat, mutta järjestelmän kunnossapito voi tapahtua muualla. Esimerkkiratkaisu pitää viraston viestintäprosessin teknisesti niin häiriöttömänä kuin mahdollista, mutta antaa mahdollisuuden myös erilaisiin järjestelmän kunnossapitovaihtoehtoihin.

Strategialuonnoksessa esitetään strategiseksi valinnaksi peruspalveluiden ulkoistamista kaupallisille toimijoille. Tämä herättää monessa suhteessa ihmetystä, kun kuitenkin luvussa 3.4 ulkoistuksen todetaan olleen oletusarvoisena ratkaisuna huono, eikä valinnalle löydy luonnoksesta selkeitä perusteita. Sisäistä ulkoistamista käsitellään vain erikoistapauksena, vaikka se voisi kokonaisuuden kannalta tarjota merkittäviä mahdollisuuksia ja olla myös kustannustehokkaampaa. On laskettavissa, että kaupallisesti hankitun asiantuntijatyön markkinahinta IT-alalla on jopa kolminkertainen verrattuna

täysipäiväisesti työllistetyn sisäisen asiantuntijan aiheuttamiin kustannuksiin.

Ulkoistamisen yhteydessä on tärkeä huomata, että ratkaisu voi vaikuttaa sähköisen viestinnän tietosuojalain (516/2004) 3. luvun sääntelemään viestien ja tunnistamistietojen käsittelyyn joko suoraan tai välillisesti haittaavalla tavalla. Mahdolliset haitat on syytä selvittää tarkemmin ja ottaa huomioon päätöksiä tehtäessä.

IT-palvelun tuottamistavan jättäminen palvelukohtaisesti ratkaistavaksi tuntuisi viisaammalta kaupallisen toimittajan suosimisen asemesta. Näin kaikki ratkaisutavat olisivat suoraan käytettävissä ja kussakin tapauksessa voidaan valita tapaukseen sopivin ratkaisu.

Sitä, että osa kansalaisista vaatisi yhä perinteistä palveluympäristöä, ei ole syytä käsitellä uhkana tai riskinä. Päin vastoin, vaatimus perinteisen palveluympäristön säilyttämisestä tukee manuaalisten varajärjestelyjen huomiointia. Näin kunnioitetaan myös kansalaisten erilaisia valmiuksia ja mahdollisuuksia sähköisten palveluiden käyttöön. Sen sijaan yhteiskunnan yhä kasvava riippuvuus tietotekniikasta ja erityisesti Internetistä on syytä huomioida.

Viimeaikaisten uutisointien johdosta kansalaiset ovat hyvin tietoisia verkkoidentiteettiin liittyvistä hyökkäyksistä. Strategiassa esitetty hallinnon asiakkaan sähköiseen itsepalveluun liittyvä mahdollisuus tarkastaa milloin tahansa kaikki tiedot, jotka viranomaisilla hänestä on, muodostaa yksityisyyden suojan kannalta merkittäviä tietosuojakysymyksiä. Lisäksi kansalaisten luottamus sähköiseen asiointiin voi pikemminkin heikentyä kuin lisääntyä.

Myös viranomaisten tietovarastojen yhteiskäyttöisyys voi sisältää samankaltaisia riskejä kuin edellä mainittu hallinnon asiakkaan itsepalvelujärjestelmä. Näiden osalta riskejä on mahdollista pienentää käyttäjäkunnan, käyttötapojen ja käyttöpaikkojen rajaamisella.

Ammatillinen osaaminen

Luonnoksessa on ammatillisen osaamisen kannalta painotettu erityisesti ostamisen osaamisen kehittämistä. Siitä riippumatta, mikä IT-palvelun toteuttamistavaksi on valittu, ostamisen osaamista merkittävämmäksi nousee Sec-ryhmän mielestä hankinnan osaaminen. Ostaminen on ainoastaan hankintaprosessin yhden vaiheen yksi vaihtoehto. Ostamisen osaamisen tarjoaminen virastoille esimerkiksi Hanselin kautta palveluna nähdään kannatettavana.

Valtionhallinnon sisäisestä ja virastojen omasta tietotekniikkaosaamisesta on tarpeen huolehtia siitä riippumatta, miten IT-palveluja toteutetaan ja tarjotaan. Vastuuta ammattitaidon kehittämisestä ei ole suositeltavaa jättää kokonaan työntekijälle itselleen. Osaava työntekijä on työnantajan etu, ja hyvän henkilöstöpolitiikan nimissä työnantajan on aktiivisesti syytä huolehtia työntekijöidensä ammattitaidon ylläpidosta ja kehittämisestä. Muussa tapauksessa strategialuonnoksessa tiedostettu riski osaamistason laskemisesta kasvaa.

Suunnitelma rekrytoida ja palkata valtion IT-toiminnan johtamisyksikköön asiantuntijoita virastoista sisältää voimavarana vahvan julkishallinnon toimintaympäristön tuntemuksen. Toisaalta se nostaa esiin riskejä sekä valtion IT-yksikön että virastojen tasolla. On mahdollista, että virastot eivät oman toimintansa turvaamiseksi halua luovuttaa parhaita voimavarojaan muualle. Tällöin nyt luotavan toiminnan osaamispohja kärsii. Jos taas virastot luovuttavat oman osaamisensa kärkeä muualle, niiden oma toimintakyky voi näitä osin olla uhattuna. Virastojen oman toiminnan varmistamisesta on tästä syystä tärkeä huolehtia.

Tietoturvallisuus valtionhallinnossa

Tietoturvallisuus on yhtäältä ohjaamista ja sääntelemistä, toisaalta sääntelyn toteutuksen seuraamista. Se ei kosketa ainoastaan palvelujen ja prosessien komponentteja vaan koko toimintaa ja toiminnan mahdollistajia. Vaikka osa tietoturvallisuuden ohjaus- ja sääntelytoimista kuuluu tietohallintoon, ei tässä valossa kaikkea tietoturvallisuutta ole mahdollista alistaa tietohallinnolle. Lisäksi keskeisimmät tietohallinnon toimialuetta koskevat ohjaus- ja sääntelytoimet on syytä päättää tietohallintoa ylemmällä tasolla. Tämä ajatus on strategialuonnoksesta havaittavissa, mutta se voisi olla tarpeen sanoa nykyistä selkeämmin.

Julkishallinnon toiminnan strategisesti tärkeä osa on huolehtia tietoturvatietoisuudesta ja sen kehittämisestä. Sen lisäksi, että IT-palveluiden hankinnassa tietoturvanäkökulmaa on pidetty tärkeänä, tietoturvatietoisuuden merkitys voisi olla selkeämmin esillä. Käyttäjiä, ja usein myös teknistä henkilökuntaa, on vaikea saada ymmärtämään tietoturvallisuuden tarkoitus, ellei johto ilmaise tukeaan tietoturvalliselle toiminnalle ja osoita esimerkkiä omalla toiminnallaan. Nykyasussaan strategiasta ei ilmene johdon rooli tietoturvallisen toiminnan perustana eikä tietojärjestelmien käyttäjien vastuu turvallisten toimintatapojen noudattamisessa. Tietohallinnolla on merkittävä rooli myös johdon ja käyttäjien tietoturvallisen toiminnan tukemisessa.

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) koostuu eri virastojen työntekijöistä. Sillä ei ole varsinaista omaa henkilökuntaa. VAHTIn johtoryhmällä, sihteeristöllä ja hankeryhmiin osallistuvilla on ensisijainen työvelvoite kotivirastoihinsa. VAHTIn työvoimatilanne on tarpeen käsitellä ennen sen roolin laajentamista nykyisestä esimerkiksi sitovien tietoturvanormien määrittämisen suuntaan.

Selvää on, että yksi VAHTIn tehtävistä on avustaa tietohallintoa. Sen toimialueeseen kuitenkin kuuluu kaikkien tietoturvallisuuden osa-alueiden käsittely, eikä sen rooli ja sijoitus valtion organisaatiossa tässä valossa ole ilmeinen. Tietohallinnon rinnalla on tarve laajemmin tietoturvallisuutta koordinoivalle elimelle. Samoin on huomattava, että tietoturvallisuuden seurannan objektiivisuus muuttuu kyseenalaiseksi, jos seurantavastuu määritellään taholle, jonka säädöstenmukaisuutta seurataan.

Yliopistojen erityispiirteet

Strategian ulkopuolelle on toistaiseksi jäänyt merkittäviä peruspalveluiksi listattujen IT-palveluiden käyttäjäryhmiä. Suurin osa yliopistojen, ja itse asiassa koko valtionhallinnon, olemassa olevien IT-peruspalveluiden käyttäjistä on opiskelijoita. Samoja yliopistojen IT-peruspalveluja käyttävät opiskelijat, yliopiston henkilökunta, vierailevat opettajat ja tutkijat, täydennyskoulutus sekä yliopistojen kokous- ja konferenssitoiminta. Strategisena tarkoituksena ei liene, että näistä peruspalveluja käyttävistä ryhmistä erityisesti opiskelijat sekä täydennyskoulutus-, kokous- ja konferenssitoiminnan asiakkaat käyttäisivät samaa palveluympäristöä kuin valtionhallinnon henkilökunta. Käyttäjäryhmän laajuudesta johtuen se ansaitsisi huomioinnin myös strategian tasolla.

Erityisesti tekniikan alan yliopistoissa osa tutkimuksesta kohdistuu sellaisiin järjestelmiin ja teknologioihin, jotka nyt ollaan määrittelemässä keskitetysti tarjottaviksi peruspalveluiksi. Tavoite voi sisältää riskejä sekä tutkimustoiminnalle että muiden hallinnonalojen tarpeille. Erityisesti Sec-ryhmä pyytää tarkkaavaisuutta valtionhallinnon yhteisen tietoverkon ja sen mahdollisen toteutuksen osalta. Tavanomainen viranomaistoiminta sekä opetus- ja tutkimustyö sopivat huonosti samaan tietoverkkoon.

Muita huomioita

Strategialuonnoksessa tuodaan yhtenäistämisen etuna esille mahdollisuus työtehtävien suorittamiseen riippumatta toimipisteestä tai työntekijän fyysisestä sijainnista. Virastot tarvitsevat kuitenkin mahdollisuuden työnantajan direktio-oikeuden puitteissa itsenäisesti päättää, missä eri työtehtäviä on lupa suorittaa. Tällä on olennainen vaikutus siihen, mistä eri tietojärjestelmiä sallitaan käytettävän sekä miten eri tietojärjestelmiä voidaan yhdistää.

Strategiassa asetetaan tavoitteeksi valtionhallinnon yhteinen tietoverkko, jota käytetään myös puhelujen välitykseen. Sec-ryhmä toivoo, ettei tällä tarkoiteta yhden tietoverkon käyttämistä kaikkeen. Puhelut on yhä syytä erottaa tietokoneiden verkkoliikenteestä erityisesti käytettävyys- ja luottamuksellisuussyistä.

Puhuttaessa tunnistamisesta on tärkeä huomata, ettei tunnistaminen vielä sisällä tunnistamisen kohteen todentamista juuri siksi, joksi kohde esittäytyy. Luonnoksessa tunnistamisella tarkoitettaneen sekä tunnistamista että todentamista.

Maksaminen vaatii verkossa tapahtuessa tyypillisesti sekä tunnistamista että todentamista. Näitä kahta tarvitaan kuitenkin laajasti myös muissa toiminnoissa. Sekä maksamisessa että tunnistamisessa ja todentamisessa on kyse niin suurista kokonaisuuksista, että jo hallittavuuden vuoksi ne olisi syytä erottaa strategiassa omiksi kohdikseen. Tärkeää on, että tunnistaminen ja todentaminen tarjoavat myös maksamisen käyttöön riittävät ja kattavasti kuvatut rajapinnat.

Lisätietoja

Tähän lausuntoon liittyen lisätietoja antavat tietoturvapäällikkö Sami O. Koskinen, Teknillinen korkeakoulu (sähköposti sami.o.koskinen@tkk.fi, puh: 09-451 4742) ja tietoturva-asiantuntija Minna Manninen, Teknillinen korkeakoulu (sähköposti minna.manninen@tkk.fi, puh: 09-451 4697).

Yliopistojen Sec-ryhmän puolesta,

Sami O. Koskinen, tietoturvapäällikkö (CISSP), Teknillinen korkeakoulu

Minna Manninen, tietoturva-asiantuntija, Teknillinen korkeakoulu

Jakelu

– Valtiovarainministeriö

Tiedoksi

– Opetusministeriö
– Yliopistojen Sec-ryhmä