VALTIOVARAINMINISTERIÖ

Muistio

JulkICT

13.11.2013

Valtionhallinnon yhteistyön kehittäminen tietoturvallisuudessa

1. Tietoturvallisuuden vastuut ja tilanteesta

Valtiovarainministeriö vastaa valtion tietoturvallisuuden yleisestä ohjauksesta ja koordinoi hallinnon organisaatioiden toimintaa kansallisessa ja kansainvälisessä tietoturvayhteistyössä. Valtiovarainministeriön ohjausroolia on vahvistettu viimeaikaisen lainsäädännön, kuten valmiuslain, lain julkisen tietohallinnon ohjauksesta sekä tietoturvallisuuden arviointilain myötä. Eduskunnan käsiteltävänä olevat hallituksen esitykset eduskunnalle laeiksi julkisen hallinnon turvallisuusverkkotoiminnasta sekä valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (150/2013 ja 54/2013) täsmentävät ja vahvistavat tätä. Kyberturvallisuusstrategiassa vahvistetaan niin ikään tietoturvallisuuden vaatima poikkihallinnollinen yhteistyö ja eri toimijoiden roolit. Valtiovarainministeriössä näistä tehtävistä vastaa ylimmän johdon alaisuudessa toimiva *Julkisen hallinnon tieto- ja viestintätekninen toiminto (JulkICT).*

JulkICT-toiminto vastaa julkisen hallinnon ja valtionhallinnon tietohallinnon yleisestä kehittämisestä ja ohjauksesta sekä julkisen hallinnon tietojärjestelmien yhteentoimivuuden edistämistä ja varmistamisesta. JulkICT-toiminto huolehtii valtioneuvoston tasolla ICT:n, tietoturvallisuuden ja kyberturvallisuuden kehittämisestä ja ohjauksesta. Kansainvälinen yhteistyö on välttämätöntä Suomen kyberturvallisuuden vahvistamiseksi ja kyberosaamisen kehittämiseksi, minkä takia JulkICT-toiminto osallistuu muun muassa ICT- ja tietoturvallisuuden kansainväliseen yhteistyöhön.

Valtionvarainministeriön asettama ja johtama *Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI* toimii valtion tietoturvallisuuden yhteistyön, kehittämisen ja ohjauksen elimenä sekä käsittelee ja yhteensovittaa hallinnon tietoturvallisuuden ja kyberturvallisuuden linjaukset. Valtiovarainministeriön ohjauksen mukaan tietoturvallisuus kattaa tiedon luottamuksellisuuden ja eheyden lisäksi tiedon saatavuuden.

Valtion organisaatiot raportoivat säännöllisesti Valtiovarainministeriölle tietoturvallisuudestaan. Erityistoimia aiheuttaneita ulkopuolisia hyökkäyksiä on vuonna 2012 havainnut noin 25 prosenttia valtion organisaatioista ja noin kahdeksan prosenttia on havainnut joutuneensa kohdistetun hyökkäyksen kohteeksi. *Useimmilla hallinnonaloilla on korkea todennäköisyys jatkossakin joutua erityistoimia aiheuttavan kyberhyökkäyksen kohteeksi*.

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

Kyberturvallisuuden perusta on hyvä tietoturvallisuus. Tietoturvallisuuden laiminlyönti yhden toimijan taholta lisää koko kyberympäristön haavoittuvuutta. Yhteisillä toimintamalleilla ja ratkaisuilla sekä laajalla yhteistyöllä ja osaamisella vähennetään kyberuhkien muodostamaa riskiä. Kyberturvallisuutta kehitetään valtionhallinnossa yhteistyössä päällekkäisyyksiä välttäen sekä kustannustehokkuus ja riittävä turvallisuus varmistaen. *Päällekkäisyyksien minimoinnissa ja toimenpiteiden priorisoinnissa tärkeitä ovat VAHTI-yhteistyö ja ohjaus sekä yhteiset ICT-palvelut ja ratkaisut.*

Kyberuhkien vakavuuden keskeinen näkökulma on tietoaineiston luokitus. *Suurimmat haitat aiheutuvat, mikäli joko suojaustason I tai II salassa pidettävää tietoa vuotaa ulkopuolisille*. Suomen valtionhallinnossa 39 virastoa kaikki ministeriöt mukaan lukien on raportoinut käsittelevänsä vähintään suojaustason II kansallisia tietoja. Kansainvälisten tietoturvavelvoitteiden perusteella salassa pidettävää turvallisuusluokan II tietoa käsitellään Suomessa yhdeksällä hallinnonalalla.

On huolehdittava, että Suomessa on kyky teknisesti varmistaa salassa pidettävien tietojen sähköinen käsittely. Tähän sisältyvät kansallinen salaustekniikan osaamisen parantaminen ja eurooppalainen ICT-laitteiden ja –ohjelmistojen tuotanto sekä luokitellun tiedon sähköisen käsittelyn ratkaisut.

Kyberuhkien hallinta edellyttää hallinnonalat ylittävän yhteistyön jatkamista ja vahvistamista sekä osaamiskeskittymiä ja yhteisten ratkaisujen kehittämisen ja käytön lisäämistä. *Kokonaisvaltaisen kyberturvallisuuden kehittäminen edellyttää hallittua keskittämistä ja tehokasta johtamista, jota osaltaan edistävät hallituksen esitysten mukaiset valtiovarainministeriön alaisuuteen perustettavat hallinnon turvallisuusverkkotoiminta ja valtion yhteiset tieto- ja viestintätekniset palvelut.*

2. Tietoturvallisuus paranee ja toiminta tehostuu hallituksen esitysten mukaisilla toimenpiteillä

Valtiovarainministeriön ohjauksessa perustetaan valtionhallinnon yhteisiä toimialariippumattomia ICT-palveluja tuottava palvelukeskus (TORI) sekä hallinnon turvallisuusverkkotoiminta (TUVE).

Keskittämällä osaaminen, hallinta ja tekniikat saavutetaan nykyistä hajautettua ja itsenäisiin ratkaisuihin perustuvaa mallia merkittävästi parempi tietoturvallisuuden ja varautumisen taso. Keskitetty ohjaus, yhteinen arkkitehtuuri, yhteiset tekniset ratkaisut ja toimintatavat varmistavat kustannustehokkaan ja yhtenäisen tietoturvallisuuden kehittämisen ja ylläpitämisen.

Nykytilanteessa kaikki virastot eivät ole saavuttaneet todennetusti tietoturvallisuusasetuksen (681/2012) edellyttämää tietoturvallisuuden perustasoa. Palvelukeskuksen perustamisella vastataan tietoturvallisuuden haasteisiin merkittävästi hajautettua nykymallia paremmin.

TORI-palvelukeskuksen tarjoamien yhteisten palvelujen on noudatettava valtion tietohallinnon kokonaisarkkitehtuuria, yhteentoimivuuden kuvauk-

sia ja määrityksiä sekä niiden on täytettävä tarvittavat tietoturvallisuutta ja varautumista koskevat vaatimukset. *Tietoturvallisuuden säädösten mukainen todentaminen ja valvonta voidaan toteuttaa kustannustehokkaasti keskitetyssä mallissa.* Perustettaessa valtion yhteiset tieto- ja viestintätekniset palvelut keskitettyyn organisaatioon vahvistetaan tietoturvallisuuden osaamista ja hallintaa osana palveluja. Keskittämällä voimavarat mahdollistetaan kustannustehokkaasti yhdenmukaiset ja turvalliset toimintatavat.

Valtion johtamisen ja yhteiskunnan turvallisuuden kannalta tärkeät yhteiset palvelut turvataan kaikissa olosuhteissa hallinnon TUVE-toiminnalla. Valtiovarainministeriöön keskitetyllä strategisella, taloudellisella ja hallinnollisella ohjauksella varmistetaan toiminnallisen ja teknisen arkkitehtuurin kehittäminen, noudattaminen sekä yhteentoimivuus ja toiminnan kustannustehokkuus. *Turvallisuusverkolla poistetaan viranomaisten ja muiden toimijoiden tarve itse rakentaa ja ylläpitää turvallisuuden ja varautumisen vaatimukset täyttäviä päällekkäisiä tietoliikenneyhteyksiä, laitetiloja ja muita tieto- ja viestintäteknisiä ratkaisuja*.

Keskeisissä palveluntuottajissa (Suomen Erillisverkot Oy ja TORI-palvelukeskus) TUVE-palvelut erotetaan hallinnollisesti, toiminnallisesti ja taloudellisesti muusta toiminnasta. Tämä varmistaa, että *palvelutuotanto kyetään järjestämään ja palvelut tarjoamaan viranomaisille tarvittavilla eri tasoilla, myös ulkomailla toimiville eri hallinnonalojen TUVE:n käyttäjille*.

TUVE-toimintaa kehitetään rakentamalla EU-turvallisuusvaatimukset täyttävät palvelut. Suomi ei vielä täytä EU:n turvallisuusluokitellun tiedon sähköisessä käsittelyssä turvallisuusluokan II kriteerejä. Ulkoasianministeriön johdolla on kehitetty salausverkkoratkaisua (Salve), jolla liitetään lähetystöt ulkoministeriön ICT-infrastuktuuriin Suomessa. Salausverkkoratkaisun avulla mahdollistetaan luokitellun tiedon siirto ulkoasiainhallinnossa. Salausverkkoratkaisu on auditoitu riittämään EU III tason (confidential) tietojen siirtoon.

Hallinnonalojen yhteisessä SATU-hankkeessa tavoitteena on mahdollistaa sekä EU II tason (secret) että kansallisen II tason (salainen) tietojen siirto että käsittely. Valtiovarainministeriön johtamassa hankkeessa hyödynnetään Salven työtä ja tuloksia. SATU-hankkeeseen sisällytetään myös ratkaisujen auditointi Viestintäviraston toimesta. EU:n auditoijat tarkastavat kansalliset järjestelmät vuonna 2015. SATU-hankkeessa ulkoasianministeriön Salve-ratkaisu laajennetaan yhteiseksi ratkaisuksi ja siirretään toimimaan osana hallinnon yhteistä TUVE-palveluympäristöä.

EU-kriteerit täyttävällä palvelutuotannolla (SATU) ja ICT-palvelujen rakenteellisella keskittämisellä (TORI ja TUVE) turvataan kaikkien viranomaisten jatkuvasti lisääntyvä kansainvälinen yhteistyö sekä vastataan tehokkaimmin kasvaviin tietoturvauhkiin.

3. Valtion ympärivuorokautisen havainnointi ja reagointikyvyn kehittäminen

Valtiovarainministeriö asetti valtion ympärivuorokautisen tietoturvatoiminnan kehittämishankkeen (SecICT) 5.4.2013. Hankkeen ensimmäisen vaiheen tehtävänä on vuoden 2013 loppuun mennessä suunnitella ja pilotoida

toimintoja, joilla parannetaan havainnointikykyä ja reagointia sekä tilannekuvaa vakavissa ja laajamittaisissa tieto- ja kyberturvallisuustilanteissa. Useat hallinnonalat nojaavat kyberturvavallisuusstrategian toimeenpanoohjelman toimenpiteissään tässä hankkeessa kehitettäviin palveluihin. Myös *Viestintäviraston kyberturvallisuuskeskus tarvitsee valtionhallinnossa keskitetyn operatiivisen yhteistyöorganisaation. Tämä luodaan SecICT-hankkeen avulla laajassa yhteistyössä.*

Hanke perustuu aiempaan VAHTI-suunnitteluun ja valtion olemassa olevien hyväksi havaittujen toimintojen kokoamiseen. Kehittäminen tapahtuu yhteistyössä valtion ja yksityisen sektorin tieto- ja kyberturvallisuuden toimijoiden sekä pilottiorganisaatioiden kanssa. *Hankkeessa hyödynnetään ja edelleen kehitetään Viestintäviraston, Valtion IT-palvelukeskuksen ja Huoltovarmuuskeskuksen tuottamia palveluja.*

Hankkeen keskeisimmät ensimmäisen vaiheen hyödyt ovat konkreettisten ja kustannustehokkaiden ratkaisujen suunnittelu sekä testaaminen käytännössä sekä päällekkäisten toimintojen ehkäisy ja eri toimijoiden roolien ja vastuiden täsmentäminen.

Toteutettavilla tuotantopalveluilla parannetaan valtion keskeisiin toimintoihin kohdistuvien vakavien sekä laajavaikutteisten tietoturvapoikkeamien ympärivuorokautista ennaltaehkäisyä ja hallintaa sekä raportoidaan valtiojohdolle tarvittaessa reaaliaikaisesti. Osa ympärivuorokautista toimintaa on valtion toiminnan kannalta keskeisen tietojärjestelmien ja -verkkojen turvallisuuden tilannekuvan hallinta.