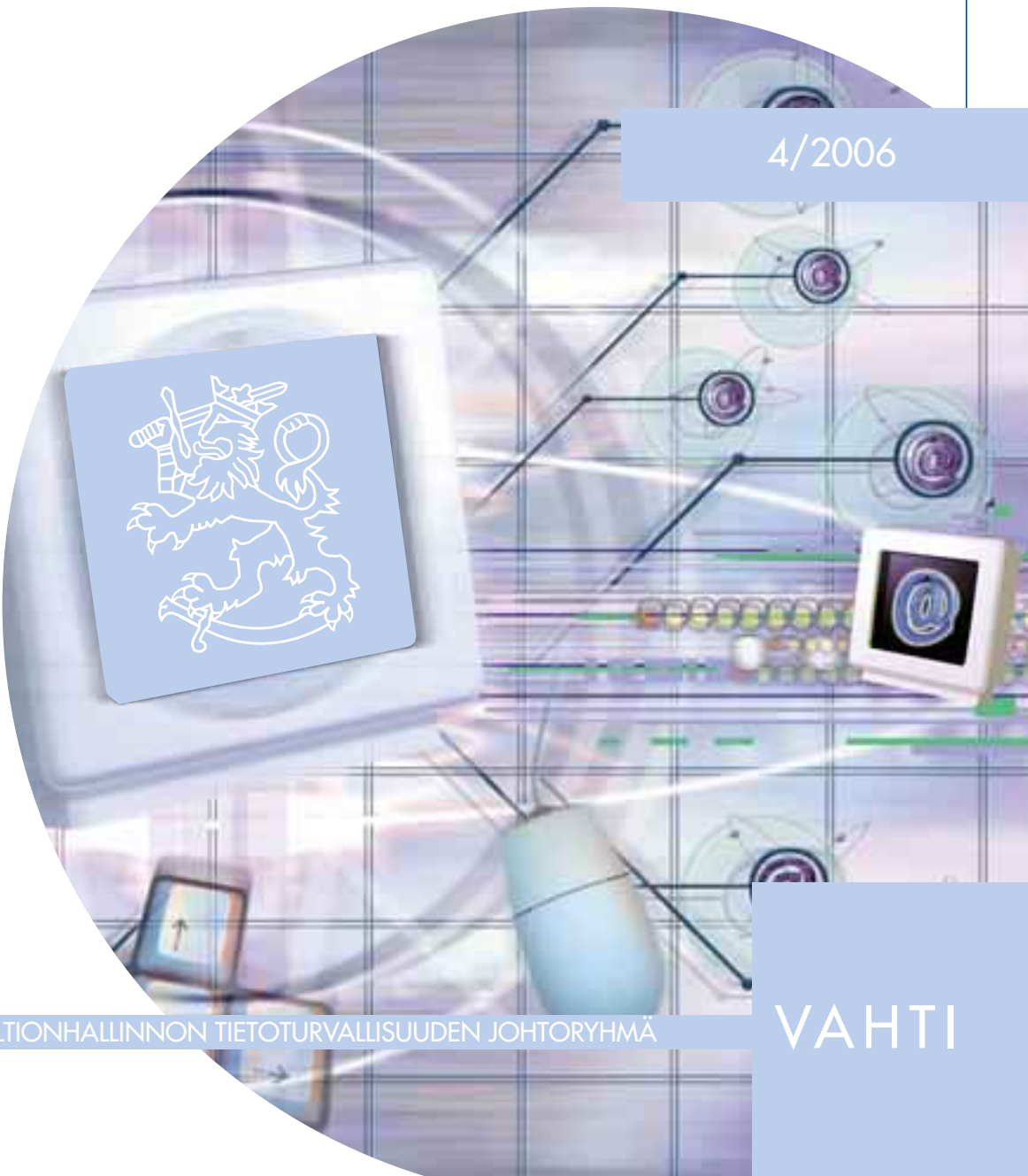
VALTIOVARAINMINISTERIÖ

SELVITYS VALTION YMPÄRIVUORO-KAUTISEN TIETOTURVATOIMINNAN JÄRJESTÄMISESTÄ



4/2006

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

SELVITYS VALTION YMPÄRIVUORO-KAUTISEN TIETOTURVATOIMINNAN JÄRJESTÄMISESTÄ

4/2006

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
Puh. (09) 160 33104

ISSN 1455-2566
ISBN 951-804-609-3 (nid.)
ISBN 951-804-610-7 (pdf)

Edita Prima Oy
HELSINKI 2006

ESIPUHE

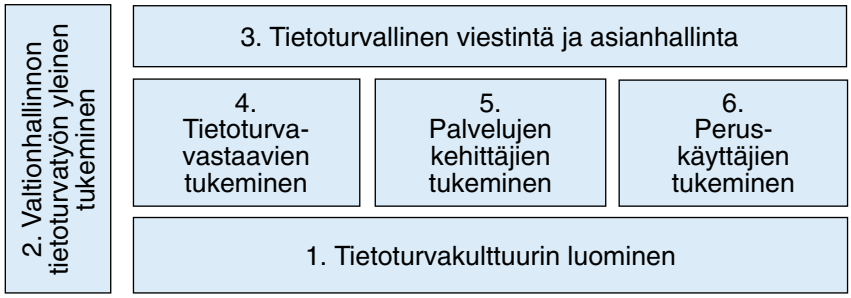
Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTIssa ovat edustettuina eri hallinnonalat ja -tasot.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat määräykset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset. Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on tunnettu muun muassa tietoturvajulkaisuista ja -ohjeista sekä tietoturvahankkeistaan (www.vm.fi/vahti).

Valtion tietoturvallisuuden kehitysohjelma on julkaistu VAHTI-julkaisusarjassa nimellä *Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006*, VAHTI 1/2004. Kehitysohjelmalla kehitetään tietoturvallisuutta laajasti osana kaikkea toimintaa. Kehitysohjelmaan sisältyy kaikkiaan 28 laajaa kehittämiskohdetta, joista osaa toimeenpannaan työryhmien tai jaostojen valmistelussa ja osaa muilla toimenpiteillä.

Kehitysohjelmaan osallistuvat laajasti kaikki hallinnonalat ja lisäksi osassa hankkeita on mukana kuntien ja elinkeinoelämän edustajia sekä ulkopuolisia asiantuntijoita. Hankkeissa on vuonna 2005 ollut mukana valtionhallintotasolla nimettyinä noin 300 osallistujaa. Osa kehitysohjelman kehitystyöstä toteutetaan hanketyöllä ja osa muulla ohjaus-, kehitys- ja yhteistyöllä. Virallisesti asetetut hankkeet löytyvät valtioneuvoston hankerekisteristä (http://www.hare.vn.fi/) VAHTIn (VM166:00/2003) alahankkeina. Seuraavassa kuvassa on esitettyinä kehitysohjelman osa-alueet.

Kaavio kehitysohjelmasta ja sen hankealueista



Tämä asiakirja on tietoturvavastaavien tukeminen- hankealueeseen kuuluvan VAHTIn alaisen valtion ympärivuorokautinen tietoturvatoiminta- työryhmän loppuraportti.

VAHTIn toiminnan kokonaisuutta vuodelta 2005 on kuvattuna VAHTIn toiminta-kertomuksessa (VAHTI 1/2006).

Sisällysluettelo

JOHDON TIIVISTELMÄ

Selvitys on ensisijaisesti suunnattu ministeriöille, valtion virastoille ja laitoksille.

Hallinnossa on laajalti kokemusta niistä vaikeuksista, jotka kohdataan, kun virka-ajan ulkopuolella sattuu viraston tietojärjestelmiin kohdistuva tietoturvapoikkeama tai kun tietoturvallisuuden ylläpitämiseen liittyvä välttämätön toimenpide on suoritettava lauantai-iltana. Työaika on muuttunut EU toiminnan vaatimustenkin myötä pidemmäksi ja ajoittain ympärivuorokauden kestäväksi (esim. EU kokoukset, kuten hallitusten väliset kokoukset). Kansainvälisiin kriiseihin ja katastrofeihin varautuminen vaatii myös jatkuvaa tietoturvallisuuden toimintavalmiutta. Tietoturvallisuuden vaaratilanteissa tietoliikenteen hätäpysäytystä viikonlopun ajaksi on joissain tapauksissa käytetty tuloksellisesti estämään viraston tietojärjestelmien vahingoittuminen.

Sama tietoturvapoikkeama vaikuttaa helposti useaan kohdeorganisaatioon, sillä virastoissa on käytössä samankaltaisia järjestelmiä ja tietotekniikkaratkaisuita. Tietokoneet, niiden käyttöjärjestelmät, oheislaitteet, tukiohjelmistot ja jopa useat viranomaissovellukset ovat samankaltaisia sekä useiden viranomaisten yhdessä käyttämiä. Esimerkiksi poliisin ja Väestörekisterikeskuksen rekisterit ovat tällaisia yhteiskäyttöisiä palveluita.

Tietoturvallisuuden vaalimisen perustarpeet ovat siis varsin samanlaisia eri valtion organisaatiolla. Valtionhallinnolla ei kuitenkaan ole tällä hetkellä kattavaa yhdenmukaista ympärivuorokautista tietoturvatilanteisiin reagoivaa palvelua.

Menossa olevien palvelukeskushankkeiden yhteydessä on mahdollista samalla rakentaa valtionhallinnon ympärivuorokautista tietoturvakyvykkyyttä. Tällöin hankkeille on oltava tarjolla riittävästi tietoturvallisuuteen erikoistunutta suunnittelutaitoa. Hankkeiden tietoturvasuunnittelijoina voidaan käyttää kaupallisia palvelun tarjoajia ja hallinnon omia asiantuntijoita esimerkiksi valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) verkostosta. Ympärivuorokautisen tietoturvatoiminnan kehittäminen ja ensimmäinen laaja tietoturvapäivystysratkaisu voi olla Valtioneuvoston kanslian raportissa 6/2004 ”Valtion tietohallinnon ohjaus ja organisointi” esitetty palvelukeskus tai yhteisesti toteutettu palvelu.

Ympärivuorokautinen tietoteknisten uhkien koordinointi ja tietoliikennetekniikan tie-

toturva-asiantuntijuus tulee perustaa Viestintävirastoon CERT-FI-toiminnan olemassa oleviin toimintoja kehittämällä.

Sen sijaan valtionhallinnon tietoverkkojen ja -järjestelmien turvaamiseen liittyviä ympärivuorokautisia käyttö- ja valvontapalvelutoimintoja tulee sisällyttää sopivien tietohallintokeskusten palvelutarjontaan. Tämä lähtökohta tulee ottaa huomioon muun muassa valtion IT-strategian toimeenpanossa ja resussoinnissa.

Pienempien yksiköiden tarpeisiin riittäviä olemassa olevia varallaolo- ja päivystyspalveluja on mahdollista kehittää henkilöstörakenteen muuttuessa tulevien vuosien eläkkeelle siirtymisten yhteydessä. Tällöin voidaan tehdä virkajärjestelyitä, joilla taataan kestävä perusta paikallisille tietoturvallisuuden varallaolo- ja päivystystoiminnoille.

Yksiköiden tietoturva-asiantuntemuksen voimavaroja voi kasvattaa myös siten, että useiden ryhmien asiantuntijat keskitetään organisaatiossa jo olevaan muuhun tukiorganisaatioon. Tukiorganisaatio voi olla esimerkiksi alueellinen palveluyksikkö tai ministeriö/esikunta. Tällaisetkin voimavarojen kohdentamiset voi toteuttaa henkilöstörakenteen muutoksen yhteydessä ilman raskaita kehityshankkeita.

Kustannuksia säästetään keskittämällä useiden valtion organisaatioiden tietoturvatoiminta yhteen palvelukeskukseen (=sisäinen ulkoistaminen).

Toimenpide ehdotukset

1. Secnet-ympäristön tietoturvapäivystys turvallisuusviranomaisille
Ympärivuorokautinen tietoturvapäivystystoiminta pilotoidaan secnet-ympäristössä ja tarjotaan myöhemmin laajemminkin valtionhallintoon, jos palvelulle on tilausta.

Ympärivuorokautinen tietoturvapalvelu hajautetaan secnet-ympäristössä kolmeen fyysiseen keskukseen seuraavasti.

- Ympärivuorokautinen asiantuntijuus toteutetaan kehittämällä CERT-FI -toimintaa.
- Ympärivuorokautinen valvonta ja
- ympärivuorokautinen operatiivinen ensivasteen toimintakyky.

Kaksi jälkimmäistä palvelua toteutetaan investoimalla lisäresursseja Poliisin tietohallintokeskuksen tietoverkkopalveluiden ja käyttöpalveluiden päivystys- ja varallaolotoimintaan sekä yhteistyössä mahdollisten muiden secnet-ohjausryhmän osoittamien tahojen kanssa.

2. Investointilaskelma valtionhallinnon tietoturvallisuuden palvelukeskuksesta
Valtiovarainministeriö asettaa työryhmän tekemään investointilaskelman valtionhallinnon tietoturvallisuuden palvelukeskuksen perustamisesta. Työryhmällä on käytettävissään mm. VAHTI:n tämä ja valtionhallinnon jaetut tietoturvaresurssit selvitys sekä toteuma tiedot Poliisin tietohallintokeskuksen budjeteista 2002–2005, sisäasiainministeriön PALKE-hankkeen toteutunut budjetti 2005 sekä näiden molempien budjettisuunnitelmat vuoden 2006 toiminnalle.

3. Kysely 24/7 tietoturvapäivystyspalveluun osallistumisesta valtionhallinnossa
VAHTI toteuttaa kyselyn siitä, onko valtionhallinnossa laajempaa tarvetta ympärivuorokautiselle tietoturvapäivystykselle. Tavoitteena selvittää 24/7-tietoturvapalvelun yleinen tarve hallinnossa, tarvittavan päivystyspalvelun laatu ja rahoituspohjan/kustannusten jakamishalukkuus kunkin mahdollisen asiakasviraston osalta.

4. Tutkimushanke tieto- ja verkkoturvallisuuden tilannekuvan monitoroinnista
Perustetaan korkeakouluvetoinen tutkimushanke valtionhallinnon ympärivuorokautisen tietoverkkojen tietoturvallisuuden tilannekuvan visualisoinnista, ensivasteen automatisoinnista ja kriisitilanteen johtamisen päätöksen teon tukijärjestelmästä. Poikkihallinnollinen tiede- ja yritysmaailmaa yhdistävä hanke toteutetaan hyödyntäen menossa olevia valtion tietohallinnon uudistushankkeita.

Secnet-hankkeeseen liittyvien turvallisuusviranomaisten tietoturvapäivystyspalveluiden toteutushankkeita hyödynnetään tutkimushankkeessa tutkimus- ja kehitysympäristöinä.

1. TYÖRYHMÄN TAVOITTEISTA JA TYÖSTÄ

Hanke on osa valtionhallinnon tietoturvallisuuden kehitysohjelmaa 2004–2006 (VAHTI 1/2004). Hankkeen tehtävänä oli selvittää tarpeet ympärivuorokautisen tietoturvatoiminnan kehittämiselle ja tehdä tarvittavat kehitysehdotukset, joilla voidaan kehittää yksiköiden kykyä nopeaan reagointiin ja tietoturvatietouden välittämiseen sekä käyttöön kellonajasta riippumatta. Selvitystyössä tuli ottaa kantaa markkinaehtoisen toiminnan hyödyntämiseen tietoturvapäivystystoiminnan toteuttamisessa. Selvityksen tuli myös rajata, miltä osin ympärivuorokautinen tietoturvatoiminta on oltava viranomaistoimintaa.

Hankkeen tavoitteeksi asetettiin esittää, kuinka hallinnossa voidaan kehittää tietoturvatilanteisiin liittyvää yhteistä reagointikykyä mm. haittaohjelmien torjunnassa, tietoturvahyökkäyksissä ja muissa häiriötilanteissa. Selvityksen tuli ottaa kantaa myös poikkeusoloihin varautumiseen liittyvän tietoturvapäivystystoiminnan kehittämiseen.

Hanke toteutettiin virkatyönä ja sen pääasiallinen työmuoto oli työpaja-muotoiset kokoukset, joita pidettiin 7 kappaletta syyskuun 2004 ja toukokuun 2005 välillä. Toissijaisena työmuotona oli sähköpostitse toimitettava tekstin viimeistely, jossa vaiheessa selvitysluonnos lähetettiin myös CERT-FI yksikölle kommentoitavaksi.

Kukin asiantuntijan työryhmään lähettänyt yksikkö huolehti omista kuluistaan. Työn ja työryhmän jäsenten aikatauluihin vaikutti valtionhallinnossa työn alla olevien tietoturvahankkeiden määrä ja henkilöiden osallistuminen useisiin samanaikaisiin hankkeisiin varsinaisten virkatehtäviensä ohessa. Työryhmä työskenteli 16.9.2004–31.5.2005 välisen ajan.

Puheenjohtaja
hallintopäällikkö Aaro Hallikainen, Poliisin tietohallintokeskus

Jäsenet
hallitusneuvos Aulis Gerlander, Sisäasiainministeriön poliisiosasto
järjestelmäasiantuntija Jari Huhtamäki, Liikenne- ja viestintäministeriö
tietojärjestelmäpäällikkö Kari Keskitalo, Kauppa- ja teollisuusministeriö

tietoturvapäällikkö Mats Kommonen, Turun yliopisto
osastopäällikkö Terho Rintanen, Puolustusvoimien tietotekniikkalaitos,
10.11. alkaen Pekka Tulokas, Pääesikunta.

Sihteeri
tietoturvallisuusasiantuntija Juhani Sillanpää, Valtiovarainministeriö

VAHTI käsitteli ja ohjasi ryhmän työtä kokouksissaan 23.9., 16.12.2004 sekä 3.3. ja 9.6.2005. Hanke esiteltiin 9.12.2004 valtion hallinnon tietoturvapäivässä. Työryhmän esitys loppuraportiksi toimitettiin VAHTI-ryhmälle 1.7.2005 verkkosivuilla kommentointia varten. Selvitysluonnos esiteltiin VAHTI:ssa 3.11.2005 ja selvitys viimeisteltiin saatujen kommenttien mukaan sen jälkeen.

Puheenjohtaja esittää suurkiitokset kaikille työhön paneutuneille sekä erityiskiitokset oikolukemisesta Sami Koskiselle, Tekninen korkeakoulu. Toteutushankkeet saakoot työstämme lähtölaudan.

2. JOHDANTO AIHEESEEN

Valtionhallinnon toiminnassa tietoturvallisuudella on keskeinen merkitys. Tietoturvapoikkeama (tietoturvaloukkaus, tietoturvavahinko, haitanteko, tietorikos tms.) voi sattua minä kellonaikana ja päivänä tahansa. Hallinnossa on laajalti kokemusta niistä vaikeuksista, jotka kohdataan, kun virka-ajan ulkopuolella sattuu tietoturvaloukkaus virastoa kohtaan tai kun tietoturvallisuuden ylläpitämiseen liittyvä välttämätön toimenpide on suoritettava viikonloppuna ilta-aikaan.

Työtehtäviin käytettävä aika on EU:n myötä laajentunut perinteisestä virka-ajasta ja ajoittain jopa 24 tuntia vuorokaudessa kestäväksi (esim. EU kokoukset, HVK). Lisäksi esim. kansainväliset kriisit (Irakin sota, Bosnian sota) vaativat jatkuvaa valmiutta. Lisääntyvä kansainvälinen yhteistyö asettaa siis vaatimuksia tietojärjestelmien jatkuvalle käytettävyydellekin.

Ympärivuorokautinen tietoturvapalvelu voi koskea myös verkkoliikenteen tai tietojärjestelmän hätäpysäytystä. Joissakin aiemmissa tietoturvallisuuden vaaratilanteissa tällaista hätäpysäytystä on jo käytetty tuloksellisesti estämään viraston tietojärjestelmien vahingoittuminen (esim. SQL-slammer -haittaohjelman torjunta).

Pikainen tietoturvapalvelun tarve voi koskea tuotteiden päivityspakettien tarkistamista. Jos päivityspaketti saapuu perjantai-iltana, niin sen asennettavuuden tarkistaminen viraston käyttöympäristöön saattaa vaatia viikonlopputyötä. Myös ratkaisutoimittajilta tai tietoturvallisuuden ensivaste-viranomaisilta (CERT-toimijat) saaduista tiedotteista voi olla syytä ilmoittaa heti viraston avain-henkilöille.

Suomen aikavyöhyke (normaaliaika UTC+2, kesällä UTC+3, Universal Time Coordinated) antaa Suomen tietoturvatoiminnalle joissain tietoturvavaaroissa toimintaedun. Haittaohjelma-epidemiat ovat monta kertaa saaneet alkunsa Kauko-Idästä tai Amerikoista, jolloin suomalainen tietoturvatoimija on saanut aikaa suojatoimille esimerkiksi aikavyöhyke-erosta johtuvan virka-aika- tai viikonlopun eron verran. On samalla syytä muistaa, että haittaohjelma-pandemiat voivat levitä yli koko internetin vain joissakin kymmenissä minuuteissa. Tällöin aikavyöhyke-erolla ei juuri ole merkitystä. Haittaohjelmien nopea leviäminen globaalisti vaatii tietoturvatoimijoilta nopeaa reagointi kykyä.

Riittävän teknisen tietoturvavasteen tarjoaminen tietoverkkojen kautta leviäville uhkille vaatii nopeaa toimintavalmiutta virka-ajan ulkopuolella. Mitä verkottuneemmassa ympäristössä hallinto toimii ja mitä tiiviimpää kansainvälinen tietojärjestelmiä hyödyntävä yhteistyö on, niin sitä tärkeämpi on hallinnon tosiasiallinen kyky torjua tietoturvallisuutta vaarantava tilanne milloin tahansa.

Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut. Tällaisia poikkeamia turvallisuustilanteeseen ovat kaikenlaiset epätoivottavat tapahtumat, jotka estävät tieto- tai viestintäjärjestelmien käyttöä, aiheuttavat päätöksen tekoon käytettävien tietojen vääristymistä, mahdollistaisivat hallinnon tietojärjestelmien tietojen asiattoman käytön tai muuta haittaa viranomaisen tietohuollolle.

Tietoturvaongelma tyypillisesti vaikuttaa useaan kohdeorganisaatioon, sillä virastoissa on käytössä paljon samankaltaisia järjestelmiä ja tietohallintoratkaisuita. Tietokoneet, niiden käyttöjärjestelmät, oheislaitteet, tukiohjelmistot ja jopa useat viranomaissovellukset ovat samanlaisia tai ainakin samankaltaisia. Tietoturvallisuuden vaalimisen perustarpeet ovat siis varsin samanlaisia eri valtion organisaatiolla.

Toisaalta virastoilla on myös eritasoisia tietoturvapalvelutarpeita: joillekin virastolle välitön reagointi on tarpeellinen, toisille taas riittää tiedotus kriittisistä haavoittuvuuksista. Ympärivuorokautista tietoturvapalvelua tarjoavan toimijan on pystyttävä räätälöimään palvelutarjontaansa erikokoisten ja eritasoisten asiakasorganisaatioiden vaatimusten mukaan.

Näiden toiminnallisten haasteiden voittamiseksi tarvittavia toimenpiteitä selvitetään tässä hankkeessa. Valtionhallinnolla ei ole tällä hetkellä kattavaa ympärivuorokautista tietoturvatilanteisiin reagoivaa palvelua. Itse asiassa harvalla virastolla on minkäänlaista omaa palvelupäivystystä. Palvelupäivystys vaatii pelkästään lakisääteisten työaikojen noudattamiseksi 7–8 hengen tiimin.

On myös huomattava, että useimmissa virastoissa virastoaikojen ulkopuolelle ulottuva päivystys aiheuttaisi tietohallintoresursoinnille huomattavia korotuspaineita, koska useimmiten ylläpidolliset tehtävät on määrätty pienelle työntekijäjoukolle, ehkä vain muutamalle henkilölle. Aamusta iltaan ulottuva etäpäivystys tai varallaolo vaatii myös laajaa tiimiä (5–10 henkilöä), koska muutoin työn henkinen sitovuus alkaa kuluttaa ja rasittaa työtehoa vähentyneen vapaa-ajan ja irrottautumisen vaikeutumisen vuoksi.

Liian pienellä henkilöstöllä pyöritettävä kiiretyövalmius alkaa ennen pitkää näkyä lomien ja vapaa-ajan käyttämisenä työtehtäviin. Jatkuessaan tällainen kuormitus alkaa aiheuttaa lisääntyvää sairastuvuutta ja työn tuloksellisuuden alenemista. Pitkään jatkuessaan ja työajan venyttämisen muodostuessa vakiintuneeksi tavaksi työterveydellisen riskit kasvavat ja tilanne vaikuttaa koko organisaation työviihtyvyyteen. Valtionhallinnossa noudatettavat työsopimukset asettavat omat reunaehtonsa työajan joustoihin.

Jos virastokohtaisella päivystäjällä on taustavoimanaan asiantunteva organisaatio, joka analysoi uhkia ja hälyttää tarvittaessa, päivystäjään kohdistuva henkinen paine keve-

nee oleellisesti. Päivystysyhteistyö eri viranomaisten ja kaupallisten toimijoiden kanssa voi olla osa ratkaisua, varsinkin jos vastuujaot ja päivystysvuorojen kierrot on mahdollista määritellä olemassa olevan lainsäädännön ja toimintavelvoitteiden puitteissa. On myös huomattava, että tietoturvapäivystyspalvelun on oltava osapuolten kannalta neutraali ja viranomaisilla on sellaisia velvoitteita, joita ei voi siirtää toiselle osapuolelle. Tällaisia siirtämättömiä velvoitteita ovat mm. valmiussuunnitteluun ja vaikeutuneisiin yhteiskunnallisiin oloihin varautumiseen liittyvät velvoitteet.

Kriittinen tietoturvapalvelu voi olla yhteen palveluntarjontaorganisaation keskitetty tai se voi muodostua usean palveluntarjoajan yhdessä muodostamasta päivystyspalvelusta. Mikäli valtionhallinnolla olisi yksi keskitetty vastuuorganisaatio tai tietoturvapalvelun ohjaamiseen erikoistunut johtoryhmä, niin se saattaisi auttaa rakentamaan valtion hallintoa yleisesti palvelevat tietoturvapäivystyspalvelut. Keskittämisestä saatu hyöty mahdollisten päällekkäisten toimintojen välttämisessä aiheuttaa koordinointityötä ja tuloksellisen tietoturvapäivystyksen rakentaminen vaatii joka tapauksessa nykyistä enemmän tietoturvatoimintaan kohdistettuja taloudellisia ja asiantuntijaresursseja.

3. YMPÄRIVUOROKAUTISEEN TIETOTURVAPALVELUUN KOHDISTUVAT TARPEET JA ODOTUKSET VALTIONHALLINNOSSA

Valtionhallinnon virastot, laitokset ja yksiköt voivat kaikki omassa toiminnassaan hyötyä ympärivuorokautisen palvelun tarjoamisesta; tarpeet ovat monitasoisia ja riippuvat yksikön omasta toiminnasta, sen luokituksista ja ylläpitotarpeista. Tarpeet voidaan jakaa pääpiirteittäin kolmeen kategoriaan:

1. Ympärivuorokautinen asiantuntijuus
   a. Turvapäivitystarpeiden edelleen tiedottaminen
   b. Turvapäivitysten analysointi yksikön järjestelmien näkökulmasta
   c. Raportointi liikkeellä olevista epidemioista ja uhkista
   d. Välityskanava ei-julkisille uhka-analyyseille ja ennakkotiedotteille
   e. Tekninen konsultointi epäillyissä tietoturvaloukkauksissa

2. Ympärivuorokautinen operatiivinen toiminta,
   a. Ylläpito
   b. Turvavalvonta (laitteistollinen ja tietoliikenteellinen)
   c. Huolto
   d. Liikenteen rajoitus ja katkaisu tarvittaessa
   e. Uudelleenohjaukset häiriötilanteissa
   f. Reagointikyky myös muihin poikkeustilanteisiin

3. Ympärivuorokautinen valvonta,
   a. Hälytyspalvelu
   b. Liikenteen analysointi
   c. Heikkouksien etsintä
   d. Uudelleenohjauksien testaaminen
   e. Turvatiedotteiden vastaanotto ja välitön analysointi

Kohdan 1 palvelut eivät edellytä jatkuvaa pääsyä kohdeviraston verkkoon, vaan ovat paikallisen tietoturva- ja ylläpitohenkilöstön tukipalveluja.

Useimmissa virastoissa on joko lukumääräisesti pienehkö ylläpitohenkilöstö, tai sitten koko tekninen ylläpito on ulkoistettu. Kuitenkaan ylläpito- ja turvallisuusvastuuta ei voida ulkoistaa, joten virastolla itsellään on oltava henkilöstöä, joka saa luotettavaa tietoa tieto-turvaa vaarantavista uhkista ja kykenee tekemään oman viraston toimintaan vaikuttavia päätöksiä uhka-analyysien perusteella. Yksinään ja pelkän julkisen aineiston perusteella paikallinen henkilöstö ei välttämättä pysy ajan tasalla ennakoitavissa olevista uhkista. Jos taustalla on keskitetty asiantunteva organisaatio, paikallinen ylläpito on huomattavan paljon paremmassa valmiudessa pitää järjestelmänsä toimintakuntoisina tilanteissa kuin tilanteissa.

Tällaista tukipalvelua ei nykyisellään vielä ole olemassa, mutta sille on akuutti tarve. Uudet, tekstiviestinä tapahtuvat varoitukset antavat jo yhden hyvän mahdollisuuden, jonka avulla virastolle tarjottua tukipalvelua voitaisiin kehittää.

Viestintäviraston CERT-FI-ryhmä on tietoteknisten ja tietoliikenteeseen liittyvien turvallisuusuhkien virallinen ja paras asiantuntijaryhmä, mutta toistaiseksi ei ole valmista mekanismia, jolla sen analyysit välittyisivät virastojen käyttöön. Toisaalta ei myöskään ole mekanismia, jolla CERT-FI saisi tietoa virastojen akuuteista tarpeista eikä myös mediaa, jolla CERT-FI voisi varoittaa virastoja uhkista, joita ei vielä voida julkaista julkisten postilistojen kautta.

Jatkuva tietoturvapäivystys mahdollistaa toiminnallisen reagointikyvyn poikkeustilanteisiin. Tietoturvapäivystykselle varatuista resursseista voidaan kriisitilanteessa luovuttaa lisäkapasiteettia muiden poikkeustilanteiden tarpeisiin. Esimerkiksi Kaakkois-Aasian katastrofin kaltaisissa tilanteissa syntyy nopea verkkotiedottamisen kapasiteetin tarve, joka voitaisiin tyydyttää jatkuvan tietoturvapäivystyksen käyttöön varatulla normaalilla ja varakapasiteetilla.

Eri virastoilla on luonnollisesti erilaiset tarpeet riippuen niiden omasta fyysisestä sijainnista ja toiminnan luonteesta. Äkkiseltään ajateltuna kohta 3 olisi luontevimmin ministeriöiden ja tärkeimpien Helsingin keskustassa tai muussa kaupungissa yhtenäisessä kampusalueessa sijaitsevien virastojen tarvitsema palvelu. Kohta 3 edellyttää sitä, että palvelun tuottaja ja asiakas ovat fyysisesti lähellä toisiaan. Verkkoja voidaan yhdistää maantieteellisesti kaukaakin, mutta laitteistohäiriöiden osalta paikalla käynti on usein tarpeellista.

Vaikkakin Helsinki on edelleen monien virastojen pääpaikka, niin palvelukeskusten sijoittaminen maantieteellisesti muuanne kuin Suur-Helsinkiin on mahdollista, perusteltua ja tukee suomalaista aluepolitiikkaa.

Turvallisuusvalvontaa voidaan sen sijaan hoitaa etäyhteyksien kautta, kun verkot on yhdistetty taatusti turvallista kanavaa pitkin (esim. luotettava, analysoitu vpn-tunneli, jonka toimivuutta ja eheyttä valvotaan katkeamattomasti). Tulevaisuudessa tällaisen turvallisen viestintäkanavan tulee tarjoamaan viranomaisten yhteinen SecNet-palvelu.

4. KOKEMUKSIA VALTIONHALLINNOSSA TOIMIVISTA PÄIVYSTYSPALVELUISTA

Valtionhallinnossa toimivat tietotekniset päivystykset palvelevat yleensä vain yhtä organisaatiota. Päivystysaika on yleensä virka-aika. Poikkeuksena löytyy kuitenkin Poliisin tietohallintokeskus PTHK ja Viestintäviraston CERT-FI yksikkö. Näiden kahden toimijan erottaa muista laajempi päivystysaika tai laajempi asiakaskunta. PTHK palvelee 24h/7vrk. CERT-FI palvelee virka-aikana, asiakkaana on kuka tahansa (tietoturvatiedotteiden vastaanotto, tietoturvan yleistieto), kuitenkin painottuen kotimaisten kieltemme takia yleensä suomalaisiin.

Päivystyspalvelut on toteutettu (pois lukien mm. CERT-FI, PTHK) normaalin virkatyön ohessa. Oman asiantuntijatyönsä ohessa päivystävät henkilöt saattavat törmätä tilanteeseen, jossa pitkäjänteiset suunnittelua vaativat työt helposti pitkittyvät ja hankaloituvat, koska päivystys vie oman osansa, vaikkei toimeksiantoja tulisikaan monta. Toiseksi, asioiden hoitaminen oman työn ohessa saattaa johtaa siihen, ettei palvelu ole aina täsmällistä ja nopeaa, asiat saattavat ”unohtua”. Toisaalta oman työn ohessa päivystämällä saadaan kustannustehokkaasti hoidettua asiakasta palveleva toiminta, eikä asiakkaan enää tarvitse tietää kuka vastaa mistäkin. Päivystystoiminnan etuna on asioiden käyntiin saattaminen tarvittaessa nopeasti ja sidosryhmien kanssa yhteydenpito on joustavampaa. Vakioitu toimintatapa helpottaa myös muita järjestelyitä, esim. lomat. Toisaalta päivystyksen ja muun organisaation väliseen tiedonkulkuun ja vastuunjakoon tulee kiinnittää erityistä huomiota henkilövaihdosten yhteydessä. Pienemmissä (1–3hlö), oman organisaation päivystyksessä ei yleensä ole mitään virallisesti rajattua vastuunjakoa, koska ei välttämättä ole henkilösidonnaisia työtehtäviä vaan tehtävät limittyvät henkilöiden kesken. Pienempää päivystystoimintaa löytyy jokaiselta taholta valtionhallinnosta. Seuraavassa kuvataan muutama esimerkki päivystystoiminnasta.

Valtioneuvoston tietohallintoyksikkö, VNTHY

Valtioneuvoston tietohallintoyksikön päivystys palvelee ministeriöitä erilaisissa yhteiskäytössä olevien sovellusten ja erilaisten tietoliikenne ongelmien ratkaisemisessa. Päivystys toimii virka-aikana, jolloin päivystysvuorossa oleva henkilö ottaa vastaa ongelman kuvauksen ja kirjaa toimeksiannon järjestelmään, jonka jälkeen päivystäjä siirtää sen oikealle asiantuntijalle hoidettavaksi, esim. vastuunalaiselle toimittajalle ja/tai VNTHYn omalle asiantuntijalle. Toimeksiannot otetaan vastaa puhelimella tai sähköpostilla. Päivystäjä myös seuraa järjestelmässä olevien avointen tapausten tilaa ja tekee niihin tarvittavat muutokset. Tapauksista, jotka koskevat myös muita kuin toimeksiannon ilmoittanutta tahoa, ilmoitetaan myös tätä kautta. Päivystysringissä on 5 henkilöä ja 2 varahenkilöä sairastapausten, lomien, kurssien sekä muita poissaolojen varten. Päivystystoiminnan keskittäminen yhden numeron taakse on helpottanut huomattavasti yhteydenottoa. Se on poistanut ongelman, jossa ei tiedetä varsinaista tahoa, johon ottaa yhteyttä. Asioiden tarpeeton siirtely eri toimijoiden välillä on poistunut.

CERT-FI, Computer Emergency Responce Team

CERT-FI vastaanottaa teleyrityksiltä tulevia tietoturvaloukkauksia ja niiden uhkia koskevia ilmoituksia. Lisäksi Viestintäviraston CERT-FI-ryhmä seuraa jatkuvasti ja maailmanlaajuisesti tietoturvallisuuden ajankohtaisia tapahtumia, tietojärjestelmiin liittyviä tietoturvallisuusongelmia ja tietoturvaloukkauksia sekä niiden ratkaisuja.

CERT-toiminnalla tarkoitetaan tietoturvaloukkauksien ennaltaehkäisyä, niiden havainnointia ja ratkaisua sekä tietoturvauhkista tiedottamista. CERT on lyhenne englanninkielisistä sanoista Computer Emergency Response Team. CERT-organisaatioita on useita ympäri maailmaa. CERT-organisaatiot toimivat yhteistyössä keskenään jakaen tietoa tietoturvaloukkauksista ja niihin liittyvistä seikoista sekä tiedottavat niistä järjestelmien käyttäjille esimerkiksi Internetin välityksellä. CERT-toiminnan päämääränä on tietojärjestelmien tietoihin kohdistuvien tietoturvaloukkauksien ja uhkien toteutumisen ennaltaehkäisy ja torjunta mahdollisimman objektiivisesti ja tehokkaasti. CERT-FI koostuu neljästä teknisestä asiantuntijasta. Viestintäviraston tietoturvallisuusyksikössä henkilöstöä on yhteensä 11. (http://www.ficora.fi/suomi/tietoturva/certtoiminta.htm)

CERT-FI mahdollistaa omien järjestelmien ylläpidon mahdollisimman tietoturvallisina. Isojen tietomassojen läpikäynti jokaisessa organisaatiossa on kallista ja resursseja vievää toimintaa, joten CERT-toiminta antaa hyödyllistä ja jalostettua tietoa eteenpäin, jolloin omien resurssien käyttö voidaan ohjata tehokkaampaan toimintaan tietoturvan ylläpitämiseksi.

Poliisin tietohallintokeskus, PTHK

Poliisin tietohallintokeskuksen tehtävänä on vastata kokonaisvaltaisesti poliisin tietohallinnosta, tuottaa ja hankkia poliisin tietotekniset palvelut sekä vastata infrastruktuurista poliisin toiminta- ja tietohallintostrategioiden mukaisesti. PTHK:n tietojärjestelmäpäivystys palvelee käyttäjiä ympäri vuorokauden jokaisena vuoden päivänä. Palveluiden käyttäjinä ja asiakasorganisaationa on myös poliisihallinnon ulkopuolisia virastoja ja laitoksia.

Osa PTHK:n palveluita on tietoverkon turvallisuusvalvonta. PTHK päivystää sisäasiainministeriön tietoliikenneverkon eräiden osien tapahtumia ympärivuorokautisesti. Operatiivinen toimintavalmius on kaikkina vuorokauden aikoina vuoden jokaisena päivänä.

Vuonna 2006 PTHK virastossa työskentelee 170 työntekijää, joista yli 90 Rovaniemen toimipisteestä käsin. PTHK:n alueellistamishanke päättyi joulukuussa 2005, jolloin kaikki Rovaniemelle siirretyt toiminnot ovat käytössä. (http://www.poliisi.fi/pthk, http://www.intermin.fi/ > Hakusana ”Poliisin tietohallintokeskus”)

Ympäristöhallinnon tietotekniikkapäivystys

Päivystyspalvelu kerää ilmoitukset käyttökatkoista, ratkaisee käyttäjien ongelmat ja valvoo palvelinjärjestelmien, tietoliikenneyhteyksien ja muiden atk-palvelujen toimintaa. Keskitetty palvelu varmistaa käyttäjille ja palveluille jatkuvan valvonnan.

Suomen ympäristökeskuksen Tietokeskuksessa on 9 henkilön päivystysrinki, joka hoitaa ympäristöhallinnon keskitettyjen atk-palvelujen ylläpidon ja neuvonnan.

(http://www.ymparisto.fi/default.asp?contentid=67807&lan=FI)

Palvelu toimii arkisin klo 8:00–16:15. Yhteyden otot tapahtuvat päivystyspuhelimeen, sähköpostiosoitteeseen tai henkilökohtaisesti.

Verohallinnon valvomo

Verohallinnon valvomossa on kokonaiskuva tietoteknisen infrastruktuurin toimivuudesta. Valvomon päätehtävänä on hoitaa keskitetysti infrastruktuuriin liittyvien häiriö- ja vikatilanteiden selvitysprosessia. Valvomo vastaa siitä, että havaittuja/uhkaavia häiriötilanteita ryhdytään selvittämään ja koordinoi käynnistämäänsä selvitysprosessia sekä tiedottaa häiriön vaikutuksista käyttäjäkunnalle. Valvomo tarjoaa muille toiminnoille yhden raportointipisteen infrastruktuurin ongelmissa. Samalla valvomo tuottaa kaikista merkittävistä tapauksista ns. jälkihoitoraportin ja tilastoi tapaukset vikarekisteriin. Lisäksi valvomo hoitaa tiettyjä rutiinitarkistuksia ja tarvittaessa käynnistää/pysäyttää palvelimia.

Tärkeimpiä yhteistyökumppaneita ovat erilaiset tekniikkaan ja sovelluksiin perehtyneet erityisasiantuntijat ja tukiryhmät. Tavoitteena on lyhentää merkittävästi vaikeiden

ongelmien ratkaisemiseen kuluvaa aikaa ja vähentää niihin kuluvaa henkilötyömäärää. Tavoitteeseen päästään selkeällä toimintaprosessilla ja hyvillä apuvälineillä siis tehokkaalla yhteispelillä.

Apuvälineinä ovat Help Desk -järjestelmä arkisin klo 7.30–16 ja päivystyspuhelin arkisin klo 7–19. Vikailmoituksia tulee kolmesta lähteestä: automaattivalvonnasta, Help Desk -järjestelmään osoitettuna tukipyyntönä tai puhelimitse.

Valvomo selvittää itse tai välittää selvitettäväksi tietoon tulleet toimintahäiriöt 20 minuutin kuluessa vikailmoituksen saapumisesta sekä päivittää tiedon häiriöstä ja sen vaikutuksista verohallinnon intranetin ilmoitustaululle. Valvomo johtaa ja avustaa vianselvitysprosessia siten, että toimintahäiriö on selvitetty ja selvityksestä tiedotettu mahdollisimman nopeasti. Tavoitteena on, että selvitysprosessi on päättynyt 3 tunnin kuluessa häiriön alkamisesta. Valvomotoimintoa hoitaa tällä hetkellä 8 henkilöä.

Ilmatieteen laitos

Ilmatieteen laitoksen operatiivisen toiminnan tehtävänä on tuottaa mm. turvallisuussääpalveluja viranomaisille ja kansalaisille. Laitoksen toiminnalla on kymmenien vuosien perinteet 24*7 / 365 operatiivisesta ympäristöstä ja sen valvonnasta, eikä tästä toiminnasta voida luopua. Laajaa sääennustustuotantoa ajetaan eri laitealustoilla ja syksystä 2005 lähtien myös omalla suurteholaskentakoneella. Ilmatieteen laitos on muuttamassa Helsingissä uusiin toimitiloihin Kumpulaan, jossa tulee olemaan nykyaikaiset katkeamattoman toiminnan edellyttämät laitetilat ja järjestelmät. Ympärivuorokautinen valvonta kattaa tuotannon toimivuuden, järjestelmien ja verkon käytettävyyden seurannan sekä tietoturvahyökkäysten sekä roskapostin monitoroinnin.

5. TIETOTURVAPALVELUN TOTEUTTAMINEN OSANA PALVELUKESKUKSEN TARJONTAA

Tässä kappaleessa tarkastellaan tietoturvapalvelun toteuttamista osana palvelukeskuksen tarjontaa ottaen huomioon mitä Valtioneuvoston kanslian raportissa 6/2004 ”Valtion tietohallinnon ohjaus ja organisointi” on esitetty. Tarkastelussa huomioidaan menossa oleva ValtIT-hanke. (http://www.valtioneuvosto.fi/vn/liston/base.lsp?r=91935&k=fi&old=754&rapo=1240, www.vm.fi/valtit)

Työryhmä on tullut siihen lopputulokseen, että valtion ympärivuorokautinen tietoturvapalvelu olisi erinomainen yksittäinen palvelu, jonka ”Valtion tietohallinnon ohjaus ja organisointi” -raportissa kuvattu palvelukeskus voisi toteuttaa osana ValtIT-hankkeessa toteutettavan palvelukeskuksen muuta tarjontaa. Se kuuluisi IT-peruspalveluiden ryhmään ja muodostaisi uutena palveluna helposti käyttöönotettavan ja pilotoitavan hankkeen. Se olisi myös merkittävä palvelu, joka omalta osaltaan edesauttaisi palvelukeskuksen palvelujen tarjontaa.

Valtion ympärivuorokautisen tietoturvapalvelun toteuttaminen aikataulullisesti sopisi myös hyvin ValtIT-hankkeen aikataulusuunnitelmiin. Vaiheen I aikana suunniteltaisiin palvelu ja toisessa vaiheessa olisi yhteisen palvelun käyttöönotto. Työryhmän mielestä kyseisen palvelun käyttöönotto olisi realistinen 1 ½ – 2 vuoden kestoisella toteutushankkeella.

Palvelun suunnittelua varten tarvitsee perustaa erillinen työryhmä, joka ratkaisee palvelun tuottamisen erityiskysymykset. Ratkaistavia asioita olisi mm. varautuminen poikkeusoloihin, kustannusten jyvittäminen mukaan tuleville organisaatioille, tietoturvapalvelujen yksityiskohtainen tuotteistaminen, nykyisten palveluorganisaatioiden hyödyntäminen, palvelun osien ulkoistaminen. Palvelun kehittäminen alusta alkaen oikeaan suuntaan edellyttäisi aluksi riittävän laadukkaan tietoturvapalvelutarpeiden kartoituksen tekemisen valtionhallinnon organisaatioihin. Tässä kartoituksessa tulisi kiinnittää huomiota niihin todellisiin palvelumuotoihin, joita mukaan tulevat organisaatiot olisivat valmiit sitovasti hankkimaan palvelukeskuksesta.

Työryhmän mielestä jatkuvan tietoturvapäivystyksen on sijaittava keskeisiltä osiltaan ja palveluiltaan valtionhallinnossa. Kokemuksien perusteella katastrofitilanteissa kaupal-

lisilla palvelutoimittajilla ei välttämättä ole tarjota lisäresursseja riittävän nopeasti eikä valtion organisaatioilla ole nopeasti irroitettavia varoja yllättävien lisäkustannusten maksamiseen. Yksikön asiantuntijoita taas voidaan komentaa tekemään virkavastuulla tarvittavia kriisitehtäviä jättämällä vähempiarvoiset rutiinitehtävät odottamaan kriisinjälkeistä aikaa.

6. KAUPALLISTEN TOIMITTAJIEN YMPÄRIVUOROKAUTISTEN TIETOTURVAPALVELUIDEN TARJONTA

Organisaatio voi ulkoistaa tietoturvatoimintaansa esimerkiksi haittaohjelma- ja roskapostisuodatuksen, palomuurin ylläpidon, hallinnollisten tietoturvapalveluiden ja joiltain osin myös päivystysluonteisten tietoturvapalveluiden osalta. On kuitenkin muistettava, että virastolla on aina vastuu ydintoiminnastaan, ja tätä vastuuta ei voi siirtää palvelun tarjoajalle. Jos organisaation on tehtävä päätöksiä tietoturvatilanteiden muutosten johdosta minä tahansa vuorokauden aikana ja minä vuoden päivänä tahansa, niin sillä on oltava oma päivystys- tai varallaolojärjestelmä, jossa virkavastuulla oleva henkilö tekee päätöksen tietoturvapoikkeamaan reagoimisesta.

Tällaisia kriisitilanteita, joissa virkamies tekee virkavastuulla päätöksiä, ovat esimerkiksi luonnonolosuhteista johtuvat poikkeamatilanteet. Tällöin virka-ajan ulkopuolella saatetaan joutua tekemään päätöksiä viraston tietoteknisien palveluiden kiiretöistä. Vaikka varsinaisen palvelutoimenpiteen tekisikin kaupallinen palvelutoimittaja, niin varsinainen päätös toimenpiteestä on tehtävä viranomaisessa, joka myös on velvollinen valvomaan toimenpiteen asianmukaisen suorittamisen.

Kaupallisten toimittajien ympärivuorokautistakin tietoturvapalvelua on saatavilla. Varsinaisen tarkemman markkinakartoituksen työryhmä jättää jatkotyöskentelyn varaan. Tietoa markkinaehtoisten toimijoiden tietoturvapalveluista saa mm. alan asiantuntijajärjestöjen kautta: FinnSecurity ry (http://www.finnsecurity.fi), Tietoturva ry (http://www.tietoturva.fi) sekä tietotekniikka-alan palveluntarjoajien kautta.

Eräissä tsunami-kriisin aikana eteen tulleissa kiireellisissä tietoteknisissä toimenpiteissä viranomainen pystyi toteuttamaan ratkaisun itse noin vuorokaudessa, kun taas kaupallisen toimijan toteuttamana ratkaisun tuottaminen olisi vienyt heidän oman arvionsa mukaan noin viikon eikä työtä olisi voitu tehdä vuodenvaihde viikonloppuna. Toimintoja ulkoistettaessa on osattava kuvata palvelutarve täsmällisesti, jotta hankinta voidaan kilpailuttaa voimassa olevan hankintalainsäädännön mukaisesti ja palvelun tarjoaja pystyy ratkaisunsa hinnoittelemaan.

On myös syytä muistaa, että kaupallisten toimittajien sopimuksissa on usein Force Majeure -pykäliä, jotka rajoittavat heidän vastuutaan tilanteissa, joissa palvelua erityisesti tarvittaisiin.

Ulkoistamisen yhteydessä on myös muistettava, että toimintojen siirtäminen oman organisaation ulkopuolelle saattaa monimutkaistaa tuotantoketjuja sekä vähentää kustannusrakenteiden läpinäkyvyyttä. Tuotantoketju voi ulkoistamisen yhteydessä tulla jäykemmäksi muutoksille kuin organisaation itsensä toteuttamana. Tällaiset ulkoistamisen vaarat ovat olemassa ulkoistettaessa viranomaisen omaa ydintoimintaa niin markkinaehtoiselle toimijalle kuin toiselle tilivirastollekin.

7. VIRANOMAISEN VASTUU YMPÄRIVUOROKAUTISEN TIETOTURVAPALVELUN TOTEUTTAMISESSA

Useille virastoille tietoturvapalvelua tuottavat yksiköt on erityisesti suojattava, koska niistä täytyy olla pääsy asiakasvirastojen ydinjärjestelmiin ja siten tietoturvapalveluyksikön vaarantuminen vaarantaa laajemman kokonaisuuden kuin yksittäisen viraston murtuminen. Henkilökunnan luotettavuuteen ja toimintakäytäntöihin tulee kiinnittää erityistä huomiota, olipa useille virastoille tietoturvapalvelua tuottava yksikkö sitten valtion virasto tai kaupallinen toimija. Asiakasvirastoissa tulee aina olla yhteyshenkilö varahenkilöineen tietoturvapalveluyksikköön päin, ja vastuujako viraston ja palveluyksikön välillä tulee selkeästi määritellä. Näin erityisesti kiireellisten hätätöiden osalta. Tällaisia hätätöitä ovat esimerkiksi viraston palveluiden tai verkkoyhteyden alasajo.

Viranomaisen toimintaa säätelevät yleislait sekä hallinnon alan erityislait. Kaikkia viranomaisia koskevia yleislakeja, joista aiheutuu velvoitteita jatkuvan tietoteknisen toimintakyvyn ylläpidolle, ovat esimerkiksi seuraavat:

- valmiuslaki (1991/1080)
- laki kansainvälisistä tietoturvallisuusvelvoitteista (2004/588)
- sähköisen viestinnän tietosuojalaki (2004/516)
- laki sähköisestä asioinnista viranomaistoiminnassa (2003/13)

Vastaavanlaisia tiettyä hallinnonalaa ohjaavia erityislakeja taas ovat vaikkapa seuraavat.

- laki eräiden alusten ja niitä palvelevien satamarakenteiden turvatoimista ja turvatoimien valvonnasta (2004/485)
- laki henkilötietojen käsittelystä poliisitoimessa (2003/761)
- radiolaki (2001/1015)
- hätäkeskuslaki (2000/157)

Muita tietojärjestelmiä, verkkopalveluita sekä viranomaistoimintaa sivuavia lakeja, joista voi myös katsoa aiheutuvan velvoitteita tietoturvallisuuden jatkuvalle vaalimiselle, ovat mm. seuraavat.

- laki tietoyhteiskunnan palvelujen tarjoamisesta (2002/458)
- laki viranomaisten toiminnan julkisuudesta (1999/621)
- henkilötietolaki (1999/523)
- ja viime kädessä myös Suomen perustuslaki (1999/731)

Päivystys- ja varallaolotyön organisoimisessa on syytä huomioida myös työsuojeluun liittyvät lait ja asetukset, joita ovat mm. seuraavat.

- työterveyshuoltolaki (2001/1383)
- laki työsuojeluhallinnosta (1993/16)
- valtion virkaehtosopimusasetus (1987/1203)
- laki työsuojelun valvonnasta ja muutoksenhausta työsuojeluasioissa (1973/131)
- työehtosopimuslaki (1946/436)

Päivystys- ja varallaolotyön toteuttamisessa tulee huomioida hankintalainsäädäntö.

- laki julkisista hankinnoista 23.12.1992/1505

Ns. Teckal-kriteerien (Euroopan yhteisön tuomioistuimen Teckal-ratkaisun seuraukset) ”sidosyksikkö-hankinta”-periaatteen vaikutus hankintatoimeen sekä hankintalainsäädännön odotettava kiristyminen johtavat hankintojen monimutkaistumiseen. Teckal-kriteerien mukaan kilpailuttamisvelvoitetta ei synny, jos hankkija valvoo yksin tai yhdessä muiden hankintayksiköiden kanssa sidosyksikköä samaan tapaan kuin omia toimipaikkojaan ja jos sidosyksikkö toimii pääosin vain omistajansa kanssa.

Jos tällainen hankintayksiköiden yhteisesti omistama sidosyksikkö myy palveluja vain omistajilleen, tai ainoastaan vähäisessä määrin ulkopuolisille, niin Teckal-kriteerit täyttyvät ja kilpailutusta ei tarvita. Jos palveluita myydään huomattavasti myös omistajatahojen ulkopuolelle, niin kilpailuttamisvelvoite syntyy. Samoin, jos yksikössä, josta hankitaan, on yksityistä omistusta mukana, niin kilpailuttamisvelvoite syntyy silloinkin.

Mikäli ympärivuorokautista tietoturvapalvelua on tarkoitus tarjota palvelukeskusmaisesti, niin sen omistajatahot ja palvelun asiakkaat on huolellisesti suunniteltava hankintalainsäädännön kannalta tarkoituksen mukaisella tavalla. Julkisesti rahoitetun palvelukeskuksen ajautuminen kilpailuttamistilanteissa kaupallisten toimijoiden markkinoille voi johtaa vaikeisiin hankintalainsäädännön tulkintoihin.

Jatkuvan verkkopalvelun tarjolla olon periaate velvoittaa viranomaista pitämään tietotekniset asiointipalvelunsa aina sellaisessa kunnossa, että kansalainen voi esteettä nii-

tä käyttää. Palvelun jatkuva tarjolla olo asettaa paitsi tietoteknisille ratkaisuille itselleen korkeita laatuvaatimuksia mutta myös kovia vaatimuksia tietoturvapoikkeamiin reagoimiselle. Vuoden 2004 aikana ja erityisesti joulukuun tsunami-kriisin aikaan valtionhallinnon tietohuollolle tuli eteen tilanteita, joissa onnistuminen edellytti virka-ajan ulkopuolista päivystys- tai varallaolotoimintaa nimenomaan tietoturva-asiantuntijoilta.

8. KUSTANNUKSET JA TULOSOHJAUS

Esitetyt kulurakenteet ovat ajateltu budjettivirasto-mallin mukaan. Tilaaja-tuottaja-mallit ja ostopalveluiden hyödyntäminen jätetään varsinaisen investointilaskelmien ja niiden vertailun tekijälle, sikäli jos ympärivuorokautisen päivystystyön katsotaan valtionhallinnossa tarvitsevan tätä selvitystä laajempaa valmistelutyötä. Tarkastelu painottuu henkilöstökuluihin, sillä palkkakulut/henkilöresurssien saatavuus on koettu käytännön toiminnassa akuutiksi ongelmaksi.

Ympärivuorokautinen päivystystyö vaatii toimiakseen 7–10 henkeä, jotta lakisääteiset työajat toteutuvat. Vähintään kolmen hengen jatkuva toimintavalmius vaatii yli 20 henkeä. Kolmessa vuorossa kolme henkeä tarvitsee vuorokauteen 9 operoijaa sekä lisäksi hallinto- ja esimieshenkilöstöä. Jotta työehtosopimusten mukaiset loma- ja lepoajat saadaan toteutettua, niin ryhmässä tulee yhteensä olla 20–30 henkeä.

Henkilöstökustannukset sivukuluineen olisivat tuollaisella ryhmällä suuruusluokaltaan 1,5 M € vuodessa, jonka lisäksi tulee laskea erityisammattitaidon ylläpitoon kuluvat koulutusinvestoinnit. Tällaisen ryhmän henkilöstökulut eivät ole lisäkustannus, jo nämä työt on joka tapauksessa jotenkin tehtävä.

Kulurakenteen määrittämisessä voi käyttää tukena jokahetkisiä tietoturvatoimintoja jo toteuttavien organisaatioiden budjetteja. Esimerkiksi Poliisin tietohallintokeskuksen toteutuneet budjetit 2002–2005 sekä budjettisuunnitelma 2006 soveltuvat tällaiseen tarkasteluun.

Kulurakenteen määrittäminen tietoturvallisuus investointivaihtoehtojen vertailuun kovin tarkasti on hankalaa ja ei välttämättä kovin tarpeellistakaan. Varsinaiset tietoturvallisuuteen käytetyt kulut kun eivät helposti ole eroteltavissa kokonaisbudjeteista. Ja vaikka keskitetyssä tietoturvapalvelukeskuksessa toteutettaisiinkin tietoturvapalvelua useille organisaatioille, niin joka tapauksessa yksiköille itselleen tulee jäämään aina omaa tietoturvatoimintaa.

Jatkotoimenpiteistä päättämisen kannalta toiminnan kustannusvaikutusten riittävä esittäminen ja vaihtoehtoanalysointi jäävät jatkotyöskentelyn varaan. Kustannusrakennetta on tässä kuvattu vain henkilöstökustannusten (palkat, sivukulut) ja koulutuskustannusten

pohjalta. Yleistä kustannusrakennetta voidaan analysoida nyt menossa olevien palvelukeskushankkeiden 2005–2006 toteutuvien budjettien pohjalta. Tällainen hanke on esimerkiksi sisäasiainministeriön talous- ja henkilöstöhallinnon palvelukeskushanke (PALKE), jossa perustettiin uusi koko hallinnonalan palvelukeskus Joensuuhun.

PALKE-hankkeen avulla on mahdollista saada tarkempaa tietoa esimerkiksi palvelutoiminnan pystyttämiseen ja tuottamiseen liittyvistä menoeristä kuten kiinteistö/vuokramenoista, atk- ja kalustokustannuksista tai puhelin-, verkko-, tietoliikenne ja tietojärjestelmäkustannuksista. Alkukustannuksia syntyy myös toimintojen siirtämiseen ja perustamiseen liittyvistä henkilöstöjärjestelyistä.

Vertailukohtana voi käyttää myös tekstissä aiemmin esimerkkinä käytetyn Valtioneuvoston tietohallintoyksikön (VNTHY) kustannuksia. Siinä työskentelee 30 henkilöä, josta vuonna 2004 kertyi 1,6 M palkkakustannukset sivukuluineen. Toteutuneet kokonaiskustannukset olivat vuonna 2004 n. 6,9 miljoonaan euroa.

Voitaneen arvioida, että vastaavan tyyppistä ja -kokoista palveluorganisaatiota esimerkkinä käyttäen 20–30 henkilöä työllistävät virka-aikana toimivat tietoturvapalveluyksikön vuotuiset kustannukset olisivat n. 5–7 M €. Mikäli toiminta olisi ympärivuorokautista, kustannukset olisivat sitä suuremmat mitä suurempi osa henkilöstöä toimii vuorotyössä. Liitteessä 1 esitetään lisää esimerkinomaisia laskelmia päivystystoiminnan vaikutuksista henkilöstökustannuksiin.

Esimerkki viidestä virastosta

Esimerkkitilanteena olkoon 5 merkittävää virastoa, joilla kaikilla on tarve 24/7 palvelevaan tietoverkon turvallisuuden valvontaan ja tietoturvajärjestelmien (haittaohjelmasuojaus, tunkeutumisen esto) käyttöpalveluun. Mikäli jokainen virasto miehittää 7–10 hengen ryhmän omiin työtiloihinsa, niin tarvitaan 5 työtilaa viisine laitteineen tietoturvapäivystykselle sekä noin 50 asiantuntijaa.

Jos viidelle virastolle toteutetaan yhteinen 24/7 palvelu, niin henkilöstöä tarvitaan päivystyksen vaatiman 7–10 hengen lisäksi viiden asiakasviraston tuomaan palvelumäärän ja virastojen toimialakohtaisen asiantuntemuksen tarvitsema lisämiehitys. Asiantuntijoiden määrällinen tarve olisi kuitenkin korkeintaan luokkaa puolet viidestä erillisestä palvelutoimistosta – siis esimerkissä noin 25 henkeä. Henkilöstökuluissa olisi siis tavoiteltavissa 50 % etu.

Tietoturvapäivystyksen työtiloja saatettaisiin tarvita jopa vain yksi, mutta esimerkiksi valmiussuunnittelunäkökulmat huomioiden toimipisteitä olisi kenties syytä olla kaksi. Toimipisteen koko ja siten myös toimintakustannukset olisivat siis joko samaa kertaluokkaa tai noin 2,5-kertaiset verrattuna yhden viraston omaan tietoturvapäivystyksen työtilaan. Verrattaessa viiteen erilliseen tietoturvapäivystyksen työtilaan säästötavoite toimintakuluissa voi olla jopa yli puolet erillisten toimipisteiden kuluista.

Tietoteknisten laitteiden ja ohjelmistojen hankinta- ja käyttökuluissa säästömahdollisuudet voivat olla erikoisohjelmistojen osalta 80 %, koska viiden ratkaisun sijasta voidaan hankkia yksi. Asiakaslukumääriin sidotut ohjelmistot eivät välttämättä tule sen edullisemmiksi, hankkiiko ne yksi keskitetty organisaatio viidelle asiakasvirastolle vai hankkiiko kukin virasto ne itse. Hallinta- ja käyttökuluissa on silti näissäkin ohjelmistoissa mahdollisuus saada säästöjä, kun yksi palveluorganisaatio huolehtii viiden asiakasviraston tarpeista.

Edellä käyty tarkastelu siis oletti, että viiden viraston oman tietoturvapäivystyksen sijaan toteutetaan vain yhteen virastoon yksi tietoturvapäivystys, joka palvelee näitä kaikkia viittä virastoa. Mikäli tietoturvapäivystys toteutettaisiin palvelukeskusmallilla, niin henkilöiden päällekkäisyyksien poistumisesta aiheutuva palkkakustannusten säästö kuluisi uuden palvelukeskuksen perustamiskuluihin. Investoinnin takaisinmaksuaika riippuu palvelukeskuksen koosta – kuinka paljon se poistaa virastoista päällekkäistä tietoturvapäivystystoimintaa ja toisaalta kuinka suuret alkuinvestoinnit vaaditaan toiminnan alkuun saamiseen.

Työryhmä jättää varsinaisen euromääräisen kulurakenteen sekä henkilölukumäärien tarkemman laskennan valtionhallinnon ja -talouden erityisasiantuntijoiden sekä mahdollisten toteutushankkeiden valmistelun varaan. Tarkennukset voi perustaa jo toimivien soveltuvien tietoturvallisuuspalveluiden nykyisille kuluille suhteutettuna siihen, minkä kokoisia asiakasvirastoja palvelut tulisi laajentaa käsittämään. Aiemmassa kappaleessa, joka käsitteli valtionhallinnon kokemuksia päivystyspalveluista, on lueteltu organisaatioita, joiden toiminnasta ja vuosien 2004–2006 toteutuneista sekä suunnitelluista budjeteista saadaan konkreettisia vertailulukuja.

Tietoturvaosaaminen

Tietoturvaosaamisen ylläpitoon on mahdollista käyttää valtionhallinnossa jo toimivia koulutusjärjestelmiä sekä valmiusharjoituksia kuten esim. Puolustusvoimain organisoima tietojärjestelmäalan valmiusharjoitustoiminta. Valtionhallinnossa järjestettävää tietoturvallisuuden erityiskoulutusta täydentämään on kuitenkin syytä käyttää paitsi kotimaisia koulutuskumppaneita niin myös osallistumista kansainvälisiin tietoturva-alan asiantuntijakonferensseihin. Mikäli 20–30 hengen yksikölle järjestetään jokaiselle yhden työviikon verran kotimaista erityiskoulutuspäiviä, niin kustannukset matkakuluineen ovat luokkaa 150 000 €. Ulkomaisen koulutuksen hinta on usein lähinnä matkakulujen verran korkeampi.

Kaupallinen koulutustarjonta tietoturva-alalla on laajaa ja koulutuspalveluita tarjoavien toimijoiden kanssa on mahdollista laatia räätälöityjä koulutuspaketteja, jolloin koulutuspäivät ovat oleellisesti edullisempia kuin yksittäin ostettuna.

Korkealaatuisen tietoturva-ammattitaidon ylläpitoon ja kehittämiseen on tarjolla myös

valmiita koulutusohjelmia. Tällaisten turvallisuuskoulutusohjelmien hinnat ovat suuruusluokaltaan 5–10 000 € per koulutusohjelmaan osallistuja. Koulutusohjelmat ovat tyypillisesti ammatillisia täydennys- ja pätevöitymisohjelmia. Eräitä tällaisia tietoturva-ammattilaiselle soveltuvia koulutusohjelmia ovat esim. TKK Dipolin tietoturvallisuuden- ja turvallisuusjohdon koulutusohjelmat (http://www.dipoli.hut.fi/turva/) ja Tampereen teknisen korkeakoulun turvallisuustekniikan ammatillisen erikoistumisohjelma (http://turva.me.tut.fi/pd/).

Hankinnat

Ympärivuorokautinen päivystysyksikkö voi hankkia sellaisia erikoisohjelmistoja, joiden ostaminen asiakasorganisaatioihin itseensä olisi kalliimpaa ja joiden käyttöaste asiakasorganisaatiossa olisi pieni. Tällaisia erityisohjelmistoja voivat olla keskitetyn palvelun toteuttamiseen hankittavat palomuuri-, haittaohjelmatorjunta- tai tunkeutumisenesto/havainnointi -ohjelmistot sekä tietoturvahavaintojen analysointiin ja visualisointiin käytettävät järjestelmät.

Useamman yksikön palvelu mahdollistaa kustannusten tasaamisen ja korkealaatuisen asiantuntijuuden ylläpidon. Pienessä yksikössä asiantuntijuuden ylläpito on kalliimpaa ja erikoisasiantuntija pääsee käyttämään osaamistaan liian harvoin. Tietoturvapäivystystoimintaan liittyvissä hankinnoissa keskitetyn yksikön on mahdollista saada volyymietua verrattuna useisiin pienempiin yksiköihin, jotka kukin itsenäisesti tekevät vastaavia hankintoja.

Eritysosaava yksikkö voi toimia myös asiantuntevana kilpailuttajana, jos ympärivuorokautisen tietoturvapäivystyksen toteutusta ostetaan ostopalveluna kaupallisilta toimijoilta. Tästäkin voi olla kustannushyötyä valtionhallinnolle kokonaisuutena. Kaikissa hankinnoissa on syytä huomioida hankintalainsäädännön velvoitteet. Koko hallinnolle soveltuvien ratkaisuiden hankkiminen keskitetyn kilpailuttajan kautta ei välttämättä ole aina mahdollista.

Hankintatoimessa on aina muistettava, että toiminta ei saa vääristää markkinoita ja että hankinnat on tehtävä hankintalainsäädäntöä kunnioittaen. Kun valtionhallinnon organisaatiot tekevät keskenään päätöksiä palveluiden toiselle tarjoamisesta, syntyy hankintasopimuksia. Erityisesti säädellyt viranomaistoiminnot ovat hankintalainsäädännön ulkopuolella, mutta muilta osin hankintalainsäädäntö pääsääntöisesti pätee erillisten oikeushenkilöiden kesken.

Tietoturvallisuuden palvelukeskus

Mikäli ympärivuorokautinen päivystystoiminta toteutetaan viranomaisessa osana laajemman palvelukeskuksen toimintaa, niin yleishallinnolliset kustannukset ja henkilös-

tön työtilakustannukset ovat normaalin kustannuslaskennan mukaiset. Mahdolliset erityiset tietoturvatoiminnalle varattavat laitteistot saattavat vaatia lisäinvestointeja verrattuna palvelukeskuksen muuhun toimintaan. Tietoturvalaitetilat on kuitenkin mahdollista joko suunnitella osana uutta palvelukeskusrakennusta tai varata tilat korkeaa turvatasoa edustavilta laitetilapalvelujen tarjoajilta. Tällainen laitetilapalvelujen tarjoaja on mm. Huoltovarmuuskeskus (http://www.nesa.fi/).

Ympärivuorokautisen tietoturvapäivystysyksikön varsinainen tulosohjaus on mahdollista toteuttaa samoilla periaatteilla kuin ValtIT-hankkeessa suunniteltuille muillekin tulosohjatuille yksiköille. Työryhmä esittää, että tulosohjauksen tarkempi suunnittelu jätetään valtiovarainministeriölle ja mahdolliselle ympärivuorokautisen tietoturvapäivystysyksikön toteuttamisen suunnittelevalle jatkohankkeelle. Tietoturvatoiminnan tulosohjauksen periaatteita on kuvattu VAHTI-ohjeessa Tietoturvallisuus ja tulosohjaus (VAHTI 2/2004). Ympärivuorokautisen tietoturvapäivystysyksikön tuloasohjauksessa on mahdollista ottaa oppia esimerkiksi Poliisin tietohallintokeskuksen ja sisäasiainministeriön poliisiosaston välisestä tulossopimusmallista, jota on kehitetty vuodesta 2000 alkaen.

Ympärivuorokautisen tietoturvavasteen vaatiman operatiivisen tietoturvaerityisosaamisen keskittämien yhteen tai muutamiin hallintoa laajasti palveleviin osaamiskeskuksiin on perustamisvaiheen jälkeen kustannushyödyllistä. Hajautetussa palvelumallissa, jossa tietoturvapäivystys toteutettaisiin useassa viranomaisessa, tulee välttämättä toiminnallista päällekkäisyyttä. Turvallisuustoiminnan kannalta päällekkäisyys ei tosin ole pelkästään negatiivinen asia, vaan hallittu päällekkäisyys antaa toiminnalle redundanssia, jota tarvitaan poikkeuksellisissa tilanteissa. Tällainen hallittu päällekkäisyys on toteutettavissa rakentamalla yksi tai muutama ympärivuorokautisen tietoturvavasteen erityisryhmä eripuolille hallintoa sekä rakentamalla riittävän monia pienempiä varallaoloon tai osittaiseen päivystykseen perustuvia pienempiä paikallisryhmiä.

Tällöin ympärivuorokautiset tietoturvapäivystysyksiköt ja -ryhmät voivat jakaa osaamistaan, sovittaa yhteen hallinnon menetelmiä sekä tarjota henkilöstölle hallinnon sisäisiä urapolkuja ammatilliseen kehittymiseen. Mikäli tietoturvapäivystyksen erityisammattilaisille tarjotaan urapolkuja hallinnossa, niin siitä on kustannussäästövaikutuksia rekrytoinnin ja perehdytysvaiheen kautta.

Henkilöstökustannusvaikutukset on mahdollista toteuttaa taloudellisesti ja lisäämättä valtionhallinnon henkilöstökuluja, jos ympärivuorokautisen tietoturvapäivystyksen vaatimat virat ja toimet perustetaan pääasiassa järjestelemällä uudelleen tulevina vuosina eläköitymisen ja muun syyn takia avoimeksi tulevia virkoja. Mikäli virkoja samalla alueellistetaan, niin menossa olevista muista alueellistamishankkeista voidaan ottaa mallia virkajärjestelyiden järjestelyyn siten, että muutokset ovat kaikille osapuolille hyväksyttäviä. Tällaisia menossa olevia alueellistamishankkeita ovat mm. vuonna 2005 päättyvä Poliisin tietohallintokeskuksen alueellistaminen ja vuonna 2005 alkanut sisäasiainministeriön palvelukeskushanke (http://www.intermin.fi).

Työryhmän mielestä edellä esitettyyn perustuen ympärivuorokautiset tietoturvapäivystysyksiköt ja -ryhmät on mahdollista toteuttaa jopa siten, että valtionhallinnon kokonais-

kulut pitkällä aikavälillä pienenevät. Tällainen toteutus vaatii virkajärjestelyjä, tietoturvapäivystystoimintojen keskittämistä sekä jatkuvan ammatillisen kehityksen ohjelmien laatimista henkilöstölle. Työryhmä uskoo, että valtionhallinnon on tulevaisuudessa kohdistettava nykyistä enemmän resursseja tietoturvatoimintaan – myös ympärivuorokautiseen tietoturvapäivystykseen.

9. VALTIONHALLINNON YMPÄRIVUOROKAUTISEN TIETOTURVATOIMINNAN KEHITTÄMISEN RATKAISUJA

Selkeä tarve 24/7-periaatteella toteutettavaan jatkuvaan tietoturvapalveluun on ainakin nopeaa operatiivista reagointivalmiutta tarvitsevilla viranomaisyksiköillä. Tällaisia ovat mm. poliisi, pelastuslaitos, puolustusvoimat ja eräät terveydenhoitoalan yksiköt. Niissäkin katkeamattoman tietoturvapalvelun tarve keskittyy kunkin toimialan tiettyihin kriittisiksi luokiteltuihin tietojärjestelmiin.

Se, onko valtionhallinnossa laajempaa tarvetta ympärivuorokautiselle tietoturvapäivystykselle, jääköön erillisellä selvityksellä/kyselyllä tutkittavaksi. Jatkotoimenpiteiden laajuudesta päättäminen vaatii tietoa, jolla tarkemmin todennetaan 24/7-tietoturvapalvelun yleinen tarve hallinnossa, tarpeen laatu ja rahoituspohjan/kustannusten jakamishalukkuutta kunkin mahdollisen asiakasviraston osalta. Tällainen kysely on mahdollista toteuttaa VAHTI-toiminnan kautta.

Tietoturvallisuuden palvelukeskus voi olla joko oma, itsenäinen yksikkö tai se tietoturvallisuuden palvelukeskuksen toiminta voidaan toteuttaa kehittämällä olemassa olevien yksiköiden sisällä toimivia funktioita palvelemaan nykyistä laajempia asiakasvirastoja. Olemassa olevia tulosyksiköitä kehittämällä voidaan taloudellisesti ja nopeasti saada aikaan 24/7-palveluita. Tällöin myös vaara päällekkäisten toimintojen syntymisestä estetään.

Työryhmä esittää, että ympärivuorokautisen tietoturvatoiminnan kehittäminen ja ensimmäisen palveluratkaisun toteuttaminen liitetään tietoturvatoiminnan kannalta sopivimman hallinnon kehittämishankkeen yhteyteen siten kuin valtiovarainministeriö katsoo parhaaksi päättää.

Tietoturvallisuuden palvelukeskus on hyödyllistä toteuttaa secnet-palveluympäristöön tukeutuen. Secnet kattaa turvallisuusviranomaiset ja täten kaikkein keskeisimmät tietoturvallisuustoiminnan tarvitsijat. Tietoturvallisuustoiminta voidaan pilotoida secnet-ympäristössä ja laajentaa palvelumallia myöhemmin laajemmalle valtionhallintoon ydintoimintojen säilyessä secnet-verkossa.

Palvelukeskus voidaan hajauttaa secnet-ympäristössä esimerkiksi kolmeen fyysiseen keskukseen, joiden toiminnot voidaan suunnata erikoistumaan ympärivuorokautiseen asiantuntijuuteen, ympärivuorokautiseen operatiiviseen toimintaan ja ympärivuorokautiseen valvontaan. Secnet-työn aikataulu sopii hyvin tällaisen tietoturvapalvelukeskushankkeen toteuttamiseen.

Ympärivuorokautinen tietoteknisien uhkien koordinoinnin ja tietoliikennetekniikan tietoturva-asiantuntijuus tulee olla CERT-FI:n toiminto, joka rahoitetaan valtion budjetista vaikkapa asiakasvirastojen kautta. Näin se voisi palkata lisää henkilökuntaa ja palvella tehokkaasti myös virka-ajan ulkopuolella. Samaisesta palvelusta hyötyvät myös suomalaiset teleyritykset, jotka nykyisellään rahoittavat CERT-FI:n toiminnan sähköisen viestinnän tietosuojalain määräämän tietoturvamaksun kautta. CERT-FI:n toimintakyvyn yhtenä tärkeänä edellytyksenä on, että se toimii jatkossakin valtionhallinnon CERT-yksikkönä. Sen vuoksi ei ole missään nimessä järkevää perustaa erillistä yksikköä, joka tekisi samaa toimintoa toisaalla valtionhallinnossa.

Tietoverkkojen ja -järjestelmien turvaamiseen liittyviä ympärivuorokautisia käyttö- ja valvontapalvelutoimintoja on sisällytettävä Poliisin tietohallintokeskuksen palvelutarjontaan. PTHK tarjoaa jo nyt turvallisuusviranomaisille laajasti tietoturvapäivystystä sekä tietoverkkojen turvaamispalveluita. Osana poliisihallinnon alueellistamista PTHK toimii Rovaniemellä käynnistävänä voimana Rovaseudun turvallisuusyhteistyöhankkeissa yhteistyössä Lapin yliopiston, Rovaniemen ammattikorkeakoulun, Rajavartiolaitoksen (erityisesti sen Rovaniemelle asettuvan tietotekniikkayksikön), Puolustusvoimain, Rovaseudun kuntayhtymän sekä muiden paikallisten toimijoiden kanssa (http://www.rovaniemi.fi > ICT turvaklusteri). Tämän aluetoiminnan kehittämisessä yksi erityispalvelu voisi olla PTHK:n tietoverkkojen turvaamistoiminnon laajentaminen oleellisesti nykyisestä rakentamalla PTHK:n Rovaniemen toimipisteestä toimiva kansainvälisesti esimerkillistä osaamistasoa oleva tekninen tietoverkkojen turvaamispalvelu laajaa valtionhallinnon asiakaskuntaa varten. PTHK:lla tulee jatkossakin olemaan suurissa taajamissa ja Etelä-Suomessa toimipisteitä, joista ympärivuorokautisia tietoturvatoimintoja tukeva lähitoiminta voidaan toteuttaa.

Ympärivuorokautisien tietoturvatoimintojen toteuttamisessa tulee huomioida kansallisen tiedotustoiminnan jokahetkiset ja aikakriittiset tarpeet sekä rauhanajan poikkeustilanteissa että varsinaisissa kansallisissa kriiseissä. Toiminnan kehittämisessä ja toimintalinjoja valittaessa on syytä toimia tiiviisti Yleisradion edustajien kanssa.

Pienempien yksiköiden omiin tarpeisiin riittäviä olemassa olevia varallaolo- ja päivystyspalveluja on mahdollista kehittää pienemmilläkin taloudellisilla panostuksilla. Henkilöstörakenteen muuttuessa tulevien vuosien eläkkeelle siirtymisten yhteydessä on mahdollista tehdä virkajärjestelyitä, joilla taataan kestävä perusta paikallisille tietoturvallisuuden varallaolo- ja päivystystoiminnoille.

Yksiköiden tietoturva-asiantuntemuksen voimavaroja saattaa olla mahdollista kasvattaa myös siten, että useiden pienien ryhmien asiantuntijat keskitetään organisaatiossa jo

olevaan muuhun tukiorganisaation esimerkiksi alueelliseen palveluyksikköön tai ministeriöön/esikuntaan. Tällaisetkin voimavarojen keskittämiset voi olla mahdollista toteuttaa henkilöstön eläkkeelle siirtymisen yhteydessä ilman laajoja kehityshankkeita.

Menossa olevien palvelukeskushankkeiden yhteydessä on mahdollista samalla rakentaa valtionhallinnon ympärivuorokautista tietoturvakyvykkyyttä, mikäli hankkeilla on käytössään riittävästi tietoturvallisuuteen erikoistunutta asiantuntijuutta. Hankkeiden tietoturvasuunnittelijoina voitaneen käyttää sekä kaupallisia toimijoita (konsultteja) että hallinnon omaa asiantuntijapoolia. VAHTI-toimijoista sekä erityisesti Valtiovarainministeriöstä olisi toivottavaa olla saatavissa tukea eri hankkeille niiden suunnitellessa valtion ympärivuorokautista tietoturvakyvykkyyttä tukevia palveluratkaisuja.

Ympärivuorokautisen tietoturvapäivystyksen toteutus vaikuttaa kriisiajan toimintaan varautumiseen. Mikäli tietoturvapäivystys keskuksia on vain yksi ja se on alueellistettu, niin tilanne on poikkeusoloihin varautumisessa vaativampi kuin jos päivystyspisteitä on useita. Valtionhallinnon kriisinsietokyvyn kannalta voi olla perusteltua toteuttaa ympärivuorokautinen tietoturvapäivystys muutamaan verkottuneeseen osaamiskeskukseen perustuen ja käyttämällä tukena pieniä, eri paikkakunnilla toimivia varallaolo- tai päivystysryhmiä.

Kukin osaamiskeskus tai varallaoloryhmä voisi keskittyä johonkin erityisosa-alueeseen. Tällä tavoin hajautuksen kustannukset olisivat kohtuulliset. On kuitenkin syytä muistaa, että osittain päällekkäinen osaaminen tuo parempaa kriisin sietokykyä, vaikkakin kustannuksissa voidaan sanoa olevan päällekkäisyyttä. Mikä tahansa organisaatio, joka on viritetty resurssiensa puolesta päivittäistoiminnan kannalta minimaaliseksi ja mahdollisimman pienillä kustannuksilla toimivaksi, on aina erittäin haavoittuva muutoksille ja kriiseille. Jos joustovaraa ei ole, niin ainoa vaihtoehto tilanteen jatkuvasti jännittyessä on ratkeaminen.

Ympärivuorokautisen tietoturvapäivystys- ja varallaolotoiminnan erityisosaamisalueita ovat mm. seuraavat.

- Tieto- ja viestintäverkkojen kautta uhkaavien haittaohjelmien tunnistaminen ja torjunta
- Tietojärjestelmiin tunkeutumisen valvonta ja estäminen
- Tietoverkkojen sekä tieto- ja viestintäjärjestelmien teknisen toimivuuden valvonta ja ylläpito
- Tietoturvallisuuteen liittyvien varoitusten antaminen, haavoittuvuuksista tiedottaminen sekä toimenpideohjeiden välittäminen
- Korjausasennuspakettien koeistaminen ja levitys/saataville toimittaminen

Valtionhallinnon tietoturvallisuuden tilannekuva koostuu tietoturvallisuuteen liittyvistä ajankohtaisista tapahtumista ja tiedoista. Tällaisia ovat esimerkiksi haittaohjelmatilanne, tieto- ja viestintäverkon käytettävyys, tietojärjestelmien palvelutaso, tietoliikenteen ja -järjestelmien kapasiteetin käyttöaste, laitteiden kunto, ennakoitavissa olevat huoltokatkot

tai vastaavat, henkilöstön saatavuus työtehtäviin (”rivissä olo”), CERT-FI:n toimittama tietotekniikan sekä tieto- ja viestintäliikenteen tekninen tietoturvallisuuden yleistilanne. Tietoturvallisuuden tilannekuvan hahmottamista auttavat hyvät visualisointi- ja raportointijärjestelmät. Tämä tietoturvallisuuden tilannekuva muodostaa osan koko valtionhallinnon tilannekuvasta.

Tieto- ja viestintäverkkojen tilan visualisointi uhkaavien toimintamallien tunnistamiseksi on yksi uusi erityisosaamisen alue, jolla Suomen valtionhallinnolla voisi olla mahdollisuus kehittyä kansainvälisesti merkittäväksi osaajaksi ja uudenlaisen tietoturvatoiminnan uranuurtajaksi. Uhkakuvien visualisointi laajasti on vielä ainoastaan aivan suurimpien verkkotoimijoiden mahdollisuuksien rajoissa sen vaatimien kalliiden erityisohjelmistojen ja -osaamisen sekä suuren laskentatehon vuoksi.

Uhkakuvien visualisointijärjestelmien kehittäminen vaatii korkeimman tutkimuksen ja -opetuksen yhteistyötä yhdessä käytännön sovellusosaajien sekä ratkaisutoimittajien kanssa. Suomen valtionhallinnon tieto- ja viestintäverkot ovat suhteellisen kompakteja verrattuna moneen muuhun valtioon ja ne ovat myös vertailukelpoisen hyvää ja uudenaikaista laatua. Valtionhallinnolla on itsellään useissa eri ministeriöissä ja virastoissa monipuolista sekä kansainvälisesti laadukkaaksi noteerattua tietoturvaosaamista, ja Suomessa toimivat kaikki merkittävät kansainväliset kaupalliset organisaatiot, joissa on asian vaatimaa osaamista. Suomessa on myös omia kansallisia yrityksiä ja yrittäjiä, joilla olisi visualisointijärjestelmien kehittämiseen tarvittavia innovaatioita ja laboratorioita.

Uhkakuvien visualisointihankkeessa kannattaa hyödyntää menossa olevia tilannekuvahankkeita sekä turvallisuusviranomaisten ja puolustusvoimien jo olemassa olevaa kyvykkyyttä. Hankkeiden voimavarojen yhdistäminen kannattaa koordinoida valtiovarainministeriöstä käsin. Tällä tavoin on mahdollista saada koottua useiden virastojen tarpeiden mukaisia kattavia ja yhdenmukaisia ratkaisuja valtionhallinnolle kohtuullisilla kustannuksilla koko järjestelmän elinkaaren ajaksi.

Valtionhallinnon ympärivuorokautinen tietoverkkojen tietoturvavalvonta on mahdollista toteuttaa rakentamalla palvelu kokonaan uudenlaiseen tilannekuvamonitorointiin perustuen. Tällainen poikkihallinnollinen tiede- ja yritysmaailmaa yhdistävä hanke voidaan Suomessa toteuttaa osana menossa olevia valtiontietohallinnon uudistushankkeita. Hanke voi olla myös kansainvälinen käyttämällä hyväksi Suomen hyviä yhteistyösuhteita paitsi lähialueella niin laajemminkin. Lopputuloksena tällaisesta uhkakuvien visualisointijärjestelmään perustuvasta tietoturvapäivystyksen toteuttamishankkeesta voi syntyä kansainvälisesti merkittävä uudenlainen toimintamalli tietoturvauhkiin varautumisessa sekä erittäin toimintakykyinen operatiivinen tietoverkkojen tietoturvallisuuden päivystysyksikkö Suomen valtiohallinnon tarpeisiin vuodeksi 2010.

LIITE 1 Lähdeaineistoa

1. ”Arjen turvaa” – sisäisen turvallisuuden ohjelma, Sisäasiainministeriön julkaisut 44/2004,
   http://www.intermin.fi/sisainenturvallisuus
2. Suomen turvallisuus- ja puolustuspolitiikka 2004,
   http://www.valtioneuvosto.fi
3. Valtion tietohallinnon ohjaus ja organisointi, Valtioneuvoston kanslian raportteja 6/2004,
   http://www.vnk.fi
4. Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Puolustusministeriön julkaisuja,
   Valtioneuvoston periaatepäätös 27.11.2003,
   http://www.defmin.fi
5. Turvallisuus- ja suojelualan koulutusmahdollisuuksia,
   Orimattilan työvoimatoimiston koulutus- ja ammattitietopalvelu, lokakuu 2002
   http://www.mol.fi/tiepa/Turvallisuusalankoulutusmahdollisuuksia.pdf
6. Suomen laki,
   http://www.finlex.fi

LIITE 2 Laskelmia päivystystoiminnan kustannuksista

Tietoturvapäivystyksen työkaluiksi on käytettävissä nykyaikaisia tietoverkon- ja tietoteknisten laitteiden valvontajärjestelmiä. Järjestelmät auttavat automatisoimaan valvontatyötä, mahdollistavat automaattiset suojatoimet sekä helpottavat varsinaisten teknisten operaatioiden suunnittelua. Tietoliikenteen reaaliaikaiset järjestelmät tuottavat katkeamattomasti havaintoja operatiivisien päätöksien tekemistä varten. Teknisten laitteiden seurantaan on käytettävissä järjestelmiä, joiden avulla voidaan ennakoida huoltotoimenpiteitä sekä havaita välittömästi rikkoutumiset.

Asiantuntijapalveluidenkin automatisointiin on käytettävissä tuoreita, suomenkielisiä puheentunnistusratkaisuja, joita hyödyntäen on mahdollista ainakin osittain tarjota 24/7 asiantuntijapalveluita automaattisesti ilman ihmistyötä. Suomessa kehitetty järjestelmä pystyy tunnistamaan yksinkertaista suomenkieltä kenen tahansa puhumana. On kuitenkin syytä muistaa, että valtionhallinnossa automatisoidut asiointipalvelut tulee tarjota suomen lisäksi vähintäänkin ruotsiksi, mutta mieluummin myös muilla tarpeellisilla kielillä.

Laitteet ja ohjelmat eivät sinänsä riitä todelliseen, keskeytymättömään reagointikykyyn. Päivystyksessä on oltava ihmisiä tekemässä valvonta-automaattien havaintojen ja automaattisten reaktioiden perusteella analyyseja siitä, milloin on tarpeen ryhtyä suojatoimenpiteisiin tai vaikkapa perua automaatin suorittama ensivaste. Mikäli valvottava toiminta on laajaa ja monimutkaista, se vaatii useita henkilöitä ja silloin myös on oltava esimiestasoinen päivystäjä (”päällikköpäivystäjä”).

Myös kiireellisten resurssien kulutuspäätösten tekemiseen saatetaan vaatia päällikkötasoista päivystäjää. Kiiretilanne voi laukaista tarpeen tehdä välittömiä päätöksiä kalliisiin seuraamuksiin johtavista toimenpiteistä. Kun tällainen resurssien välittömään kulutukseen johtava kiiretilanne sattuu keskellä yötä pyhäpäivänä, niin päivystyksessä on oltava työvuorossa oleva, välittömästi parhaassa mahdollisessa työkunnossa oleva johtovastuinen henkilö, jolta voidaan edellyttää kypsää harkintaa kalliiden päätösten tekemiseen.

Pelkkä automatisointi ei siis ratkaise 24/7-tasoista palvelua vuoden jokaiselle tunnille. Henkilöstöä tarvitaan sen mukaan, miten laajasta toiminnasta on kyse. Jos päivystävää henkilöstöä on paljon, se vaatii myös päivystykselle päällikköä, jolla voi olla valtuu-

det hyvinkin radikaaleihin päätöksiin välittömän toimivaltansa puitteissa.

Tietoturvapoikkeamista johtuvien vaativien tilanteiden johtaminen on organisaatioissa onnistunut usein hyvin, koska

- tapahtumat ovat onnekkaasti alkaneet virka-ajan liukumien puitteissa,
- on tehty korvauksetonta ylityötä,
- tilannejohtoon joutuneet virkamiehet tai sidosryhmät ovat osanneet soitella tuntemilleen linjaesimiehille tai asiantuntijoille kunnes ovat jonkun tavoittaneet ja
- koska poikkeama ei useinkaan ole vaatinut useiden päivien kestoista tilannejohtajuutta ("kriisijohtamista").

Koska nimenomaan henkilöstökulut tekevät katkeamattomasta, jokahetkisestä toiminnasta kalliin, niin seuraavassa tarkastellaan päivystävän henkilöstön työnantajakuluja. Luvut ovat suuruusluokaltaan viitteellisiä ja todellisista toteutuneista henkilöstökuluista johdettuja.

A. Vaihtoehtona päivystystoiminnan kehittäminen

Johto- ja toimintavalmiutta voidaan kehittää perustuen olemassa oleviin päivystys- ja varallaolojärjestelyihin. Tämä voi olla mahdollista esimerkiksi päällystön työvuorojärjestelyin. Tällainen ratkaisu voi olla mahdollinen myös siten, että (tietojärjestelmä)päivystyksen miehitystä vahvistetaan esimiestasoisilla virkamiehillä.

Mikäli tietojärjestelmäpäivystyksen miehitystä vahvistetaan myös järjestelmäasiantuntijuudella, niin mahdollista saavuttaa parempi järjestelmäspesifinen kyky vähintäänkin joihinkin järjestelmiin myös virka-ajan liukumien ulkopuolella.

Päivystävän henkilöstön vuosikustannuksen suuruusluokka per henkeä:

- Vaativuustaso 40.07 (operointi) 35 700 €
- Vaativuustaso 40.14 (esimies) 58 000 €
- Vaativuustaso 40.17 (päällikkö) 70 600 €

Jotta päivystyksessä on aina vähintään 1 henkilö normaalit lomat ja kaikki työjaksot huomioiden, niin ryhmässä tulee olla ainakin 8 henkeä. Tällöin myös kaikkein eniten pyhäpäiviä sisältävälle (tosin harvoin allakkaan sattuvalle) työjaksolle on ainakin 1 henkilö käytettävissä.

Kustannukset 8 vuoroesimiehen päivystysryhmästä

- 8 x 58 K€ = 464 000 €

Kustannukset 8 vuoropäällikön päivystysryhmästä

- 8 x 70,6 K€ = 564 000 €

Erityisasiantuntijoiden 8 hengen päivystysryhmän kustannukset ovat samaa luokkaa kuin vuoroesimiesten.

- 8 x 58 K€ = 464 000 €

Operoinnin 8 hengen ryhmän kustannus

- 8 x 35,7 K€ = 285 600 €

On myös muistettava, että virka-ajan toiminnot eivät poistu päivystystä kehittämällä. Päivystysorganisaatio tarvitsee tuekseen virka-aikana toimivaa tulosyksikön johtoa, henkilöstö- ja taloustoimea sekä muuta viraston asiantuntijaorganisaatiota.

Taulukko 1. Kustannuslaskelma päivystykselle.

24h TOIMINTO	HENKEÄ	€ / VUOTTA
Johtovalmiuskykyinen päällikköpäivystys	8	564 000
Vuoroesimies	8	464 000
Asiantuntijapalvelu	8	464 000
Operointipalvelu	8	285 600
YHTEENSÄ	32	1 777 600

Tämä järjestely takaa jokaisena vuoden tuntina kaikkina työjaksoina normaaleilla työaikajärjestelyillä vähintään yhden hengen päällikkötason johtovalmiuden, vuoroesimiestoiminnon sekä asiantuntijapalvelun että operoinnin. Minimimiehitys lomat huomioiden, mutta ilman sairaus- tai muita poissaolojen ennakoimista, on tällöin joka hetki 4 henkeä.

Sairaus- yms. ennakoimattomien poissaolojen vaikutusta minimimiehitykseen voi pyrkiä vähentämään lisäämällä henkilöitä vahvuuteen.

B. Vaihtoehtona varallaolotoiminnan kehittäminen

Varallaolo voidaan järjestää siten, että varallaolopuhelimen tavoitettavissa on aina joku ao. varallaoloringistä. Varallaolijoiden vuorolista toimitetaan aina etukäteen palkanlaskijalle. Esimerkiksi varallaolovuoro voidaan asettaa päättyväksi maanantaina klo 8 ja vuoro alkavaksi maanantaina klo 16.15.

Virastojen johtajat (apulaisjohtajat) eivät tyypillisesti ole varallaolojärjestelyissä mukana, vaan heidät tavoitetaan tarvittaessa – viime kädessä vaikka noutamalla.

Varallaolossa olevalle maksetaan varallaolokorvausta jokaisessa palkkaluokassa. Korvaus voidaan sopia olevan tietty prosenttiosuus tuntipalkasta (laskettuna varsinaisen palkan mukaan) virka-ajan ulkopuoliselta varallaoloajalla.

Varallaolokorvaus 15% mukaan vastaa noin ½ henkilötyöviikon panosta (noin 19 ½ tunnin palkka) viikossa. Tällainen järjestely investointi siis maksaisi kahdessa vuodessa noin yhden vastaavan tasoisen viran palkkakustannusten verran.

Kun taas 25% mukaan lähes henkilötyöviikon panosta (noin 32 ½ tunnin palkka, 87%) viikossa ja noin 14 kuukaudessa investointi vastaa yhden kokopäiväisen henkilön tuntien palkkoja.

Varallaolokorvaus maksetaan siis vain varallaolosta ja varallaolovuorolla alkava työtehtävä korvataan erikseen ylityömääräysten mukaisesti.

On huomattava, että mikäli esimerkiksi lauantaina tai pyhänä varallaolija alkaa tehtävän, niin se lasketaan hänen viikkotuntityökseen. Tällöin voi käydä niin, että viikon ollessa muuten vajaa (esimerkiksi arkipyhän, sairauspoissaolon tms. vuoksi) saattaa vapaa-ajalla tehty työ jäädä normaalituntipalkkaiseksi työksi.

Ylemmissä palkkaluokissa, joissa ylityökorvausta ei ole, niin varallaolovuorolla tehdystä työstä ei tule enää lisäkorvausta.

Taulukko 2. Kustannuslaskelma varallaolosta.

VARALLAOLOTOIMINTO	% TUNTIPALKASTA	**MAKSAA YHDEN KOKOPÄIVÄISEN VIRAN VERRAN**
Varallaolo	15%	23 kuukaudessa
	25%	14 kuukaudessa

Tällainen järjestely siis takaa ainoastaan tehtävään lähtövalmiuden ja varsinaisen toiminnan kustannus tulee tämän lisäksi niissä palkkaluokissa, joissa on ylityökorvaus.

Varallaolotoiminto lepää usein sen varassa, että varallaolijalla on mukanaan/kotonaan työympäristö. Korkean turvallisuuden järjestelmien etäympäristöt tai niiden operointi kotityönä on hyvin turvallisuusperiaatteiden vastaista. Tavanomaisia järjestelmiä – jopa joitain viranomaisjärjestelmiäkin – on mahdollista sallia operoitavaksi liikkuvasta työasemasta etä-, matka- tai kotityönä tehtynä.

Suunniteltaessa korkean käytettävyyden katkeamatonta palvelua, sen kulmakivenä ei voi olla varallaolo. Varallaolojärjestelyin voidaan tukea korkean turvallisuuden ympäristöjen 24/7-päivystystä, mutta varsinainen päivystystyö vaatii sille suunniteltuja työtiloja ja varta vasten vuorotyöhön palkattua henkilöstöä.

C. Johto- ja päivystysvalmiuden kehittämisen yhteenveto

Johtovalmius- ja päivystysjärjestely, jossa varallaolopuhelimen tavoitettavissa on aina joku viraston johdosta, on mahdollista järjestää yllä olevaa soveltaen ottaen huomioon asianomaisen hallinnonalan suosittelemat yleiset johtovalmiuskäytännöt.

On suositeltavaa, että johto- ja päivystysvalmiutta kehitetään perustuen olemassa oleviin päivystys- ja varallaolojärjestelyihin. Virastojen johtajat (apulaisjohtajat) eivät yleensä ola varallaolojärjestelyissä mukana, vaan heidät tavoitetaan tarvittaessa.

Johtovalmiuskykyinen 8 hengen 24/7 päällikköryhmä maksaa vuodessa noin 0,5 M€, ja kustannukset ovat noin 128 000 € enemmän verrattuna vastaavan palkkaisiin virka-aikaa tekeviin päälliköihin. Samoilla vuosikustannuksilla saa 10 hengen virka-aikaa tekevän päällikkötasoisten virkamiesten ryhmän.

Päällikköviran varallaolojärjestely maksaa 15% tuntikorvauksen mukaan kahdessa vuodessa yhden kokopäiväisen virkavuoden verran ja 25% korvauksella jo 1 vuodessa 2 kuukaudessa yhden päällikköviran verran.

Samalla vuosikustannuksella kuin saadaan yksi varalla oleva päällikkö, saadaan yksi päivystävä operaattori töihin.

Tilannejohtovalmiutta voi parantaa kehittämällä päivystystoimintoa lisäämällä sinne esimiespäivystäjiä, joiden koulutuksessa ja tehtävissä otetaan huomioon päätösvalta ja vastuu poikkeavissa tilanteissa siihen asti kunnes johto tavoitetaan.

Esimiespäivystäjien 8 hengen ryhmä maksaa noin 0,5 M€ / vuosi.

LIITE 3 Yhteenveto selvitykseen annetuista kommenteista

Syyskuun 2005 alkuun mennessä toimitetut kommentit selvitysluonnokseen on otettu huomioon tekstissä. Lukijan toivotaan kiinnostuvan raportin sisällöstä sen kieliasun ja esitystekniikan puutteista huolimatta. Usean kirjoittajan teksteistä kootun raportin luettavuus onnahtaa, kuten monissa kommenteissa todettiin.

Raportissa käytetyt termit *”tulee”, ”on sisällytettävä”* tms. eivät sido tulevaa päätöksen tekoa. Valtionhallinnon ympärivuorokautisten tietoturvapalveluiden mahdollisessa rakentamisessa on käytettävissä erilaisia ratkaisumalleja ja tosiasiallisissa ratkaisuissa tulee ottaa huomioon kaupallisten toimijoidenkin tarjoamat mahdollisuudet.

Suuri osa valtionhallinnon keskeisistä järjestelmistä on ulkopuolisten palveluntarjoajien ylläpitämiä. Tätä kautta valtionhallinnon ympärivuorokautinen tietoturvatoiminta integroituu palveluntarjoajien tietoturvapalveluihin. Tästä aiheutuvat heijastukset tulee selvittää mahdollisien tulevien toteutushankkeiden yhteydessä, kuten myös ympärivuorokautisen tietoturvatoiminnan prosesseja kuvaavan esitysgrafiikan tuottaminen sekä kaupallisen palvelutarjonnan tarkempi selvitys.

Tulevien ympärivuorokautisia tietoturvapalveluita toteuttavien hankkeiden aikataulut on syytä tarkentaa realistisiksi hankkeiden yhteydessä. Valmisteluun kuluu päätoimisesti asiaa toteuttavalta ryhmältä vuoden verran. Palvelun kenttätestaus, jossa prosessien puutteet etsitään ja korjataan, voi viedä puolesta vuodesta vuoteen. Palvelun käyttöönottohanke voi viedä aikaa 1 ½ – 2 vuotta.

Lainsäädäntöön liittyvän jatkotyöskentelyn tulisi alkaa analyysilla mahdollisista säädöstasolla olevista puutteista tai rajoituksista, jotka vaikuttavat järkevien ja tarpeellisten tietojen luovuttamiseen. Viranomaisyhteistyön toimivuuteen liittyviä keskeisiä kohteita ovat muun muassa tunnistamistietojen ja haavoittuvuustietojen jakaminen eri organisaatioiden välillä.

Lukijaa pyydetään myös huomaamaan, että tämän selvityksen rinnalla toimitettiin erillinen selvitys valtionhallinnon tietoturvaresurssien jakamisesta. Valtionhallinnon tietoturvaresurssien jakamisesta tehty selvitys toteutettiin sillä ajatuksella, että aihepiiristä kiinnostuva lukija siirtyy sen jälkeen lukemaan tätä nyt käsilläsi olevaa selvitystä. Tämä

selvitys esittää erään mahdollisen useille valtion organisaatioille yhteisen tietoturvaresurssin – keskeytymättömän, jokahetkisen tietoturvapäivystyksen. Asiaan yleisesti liittyviä näkökulmia ei ole toistettu tässä selvityksessä, vaan lukijaa pyydetään tutustumaan tämän selvityksen kanssa samaan aikaan julkaistuun valtionhallinnon jaettujen tietoturvaresurssien VAHTI-työryhmän selvitykseen.

Alla esitetään tiivistelmä mukaan tuoduista näkökulmista. Lausujat on esitelty aakkosjärjestyksessä.

1 Ajoneuvohallintokeskus

Ajoneuvohallintokeskus pitää raportin sisältöä hyvänä, mutta huomauttaa luonnoksessa olevan paljon kielellisiä ja kirjoitusvirheitä.

2 CSC – Tieteellinen laskenta Oy

CSC Tieteellinen laskenta Oy toteaa, että ’Selvitys valtionhallinnon tietoturvaresurssien jakamisesta’ ja ’Valtion ympärivuorokautisen tietoturvatoiminnan järjestämistä koskeva selvitys’ menevät paljon päällekkäin ja toivoo kirjoittajien perehtyneen toisen ryhmän teksteihin. Näin myös meneteltiin kyseisissä ryhmissä.

CSC Tieteellinen laskenta Oy kannattaa ajatusta, että ympärivuorokautinen tietoteknisten uhkien koordinoinnin ja tietoliikennetekniikan tietoturva-asiantuntijuus tulee perustaa Viestintävirastoon CERT-FI -toiminnan olemassa olevia toimintoja kehittämällä. Esimerkiksi voitaisiin panostaa CERT-FI:n toimintaedellytyksiin neuvonnassa ja taustatukena ja lähteä kehittelemään toimintaa siltä pohjalta.

CSC Tieteellinen laskenta Oy esittää selvityksessä ehdotetun kahden keskuksen (CERT-FI, PTHK) kehittämistä siten, että näiden tietoturvatoiminnot olisivat jaettuja keskusten kesken. Tällöin vakavissa ongelmatilanteissa toinen keskuksista voisi hoitaa kaikkia tietoturvapalveluita.

CSC Tieteellinen laskenta Oy huomauttaa, että vaikkakin selvityksessä ValtIT-hankkeen aikataulua pidetään realistisena, niin tästä ei kuitenkaan ole täyttä varmuutta. Tietoturva-asioissa aktiivisimpia ovat ne, joiden dokumentaatio ja ylläpitokäytännöt ovat hyvällä tasolla, mutta kun otetaan mukaan koko laaja organisaatioiden kirjo, lienee isolla osalla puutteita omissa käytännöissään. Tietoturvatyössä pelkkä ohjeistus ei riitä vaan tarvitaan myös turva-aukkojen korjaamista ja muuta käytännön työtä.

Tietoturvatyö eroaa merkittävästi järjestelmien normaalista valvonnasta. Normaalissa valvonnassa on useimmiten kysymys ns. rutiiniasioista, joita harjoitellaan usein ja niihin voidaan varautua. Tietoturvaloukkauksissa taas suunniteltu järjestelmä on pettänyt ja ollaan ns. harmaalla alueella, josta ei ole yleensä dokumentaatiota tai toimintasuunnitelmia, koska näissä esille tulleet ongelmat on lähtökohtaisesti jo korjattu järjestelmään.

CSC Tieteellinen laskenta Oy pohdiskelee keskuksen toimintaan esitetyistä ehdotuksista seuraavaa. Selvityksessä esitetään, että vähintään kolme henkilöä olisi jatkuvassa toimintavalmiudessa. Jotta tietoturvapoikkeamatilanteissa voidaan toimia tehokkaasti, on vastuut ja valtuudet oltava määriteltyinä tarkasti. Aina ei päättäjiä ole paikalla, niin itse keskuksessa kuin palveluita käyttävissä organisaatioissakaan. Jotta viesti ja toiminta saadaan toimimaan, on riittävät oikeudet omaavaa henkilökuntaa oltava tavoitettavissa. Tämän tiedostaminen ja saattaminen käytäntöön vie aikaa.

Kansallisesti merkittävässä kriisissä kolmen hengen vuorovahvuus ei välttämättä riitä. Myös se, miten silloin saadaan 'hätävalmius' paikalle, tulee olla kirjattuna.

Rinnakkain kansallisten keskitettyjen keskusten kehittämisen kanssa tulisi huomioida myös toimintamallien ja käytäntöjen luominen yritysten ja yhteisöjen tietoturvayksiköiden kanssa. Tämä mahdollistaa sen, että ongelmatilanteissa toimenpiteitä saadaan toteutetuksi riittävän laajasti.

CSC Tieteellinen laskenta Oy toteaa, että selvityksessä esitetyt tehtävät tietoturvapäivystykselle ovat todella haastavia ja että ne sisältävät myös kaiken ylläpitotyön. Tämä herättää kysymyksen, löytyykö Suomesta 25 tietoturvan rautaista ammattilaista kolmivuorotyöhön valtion palkoilla alueellistettuun työhön? Tehtävä ei ole helppo. Tarvitaan todella rautaista osaamista. Sitä saa vain harjoittelemalla. Tähänkin tarvitaan aikaa.

CSC Tieteellinen laskenta Oy:n kommentti www-osoitteiden kirjoitusasusta huomioitiin tekstissä.

3 Huoltovarmuuskeskus

Huoltovarmuuskeskus esittää yllä mainitusta selvitysluonnoksesta lausuntonaan seuraavaa:

- HVK pitää selvityksen kohteena olevaa toimintaa tärkeänä ja kehittämisen arvoisena.
- Selvityksessä on tehty hyvää pohjatyötä mm. tarvittavien resurssien kartoittamisessa.
- Valvonnan järjestämisessä olisi syytä välttää turhaa hajauttamista. Hajauttaminen johtaa helposti päällekkäiseen työhön ja toisaalta katvealueiden syntymiseen. Asiakkaiden puolella saattaa toisaalta syntyä epäselvyyttä oikean vastuuviranomaisen löytämiseksi.
- Henkilöstöllä tulee olla riittävät toimivaltuudet ja -kyvykkyydet toimia myös äkillisen kriisin sattuessa. Tämä tarkoittaa mm. ylitöiden tekemistä, tiedotusosaamista ja yhteistyöverkoston tuntemista.
- Varautumisen ja valmiussuunnittelun kannalta on kuitenkin syytä rakentaa toiminnolle kaksi toimipistettä.
- Tietoturvapalvelun käyttämät tietojärjestelmät on syytä varmistaa esim. Huoltovarmuuskeskuksen varakeskuspalvelun avulla.

4 Ilmailulaitos

Ilmailulaitoksen mielestä selvityksessä esiin tuodut ongelmat ovat hyvin ajankohtaisia monella organisaatiolla ja se pitää hyvänä, että aiheesta on tehty selvitys.

Ilmailulaitos toteaa selvityksen olevan käytännönläheinen ja monipuolinen sekä selvityksen ehdotukset ovat sen mielestä realistisia ja toteutuskelpoisia.

5 Ilmatieteen laitos

Ilmatieteen laitos esittää lausunnossaan seuraavaa.

Ympärivuorokautisen tietoturvallisuustoiminnan kehittämisen valtionhallinnossa parantaa valtion tietoturvallisuutta. Hankkeen tavoite kehittää ympärivuorokautista tietoturvatilanteisiin liittyvää yhteistä reagointikykyä mm. haittaohjelmien torjunnassa, tietoturvahyökkäyksissä ja muissa häiriötilanteissa keskitettyjä voimavaroja käyttäen on keskeinen valtion hallinnon tietoturvallisuuden kehittämiskohde.

Keskittämisen kriteereinä tulee olla taloudelliset ja toiminnalliset perusteet. Keskitettäessä tulee varmistaa palvelujen jatkuva kehittyminen ja kustannustehokkuuden parantuminen. Tietoturvatoiminnan ympärivuorokautisen palvelun tarjoajasta tulee päättää läpinäkyvästi kilpailutuksen pohjalta ottaen huomioon taloudelliset ja toiminnalliset perusteet.

Raportissa tuotiin vahvasti esille järjestelmien ja tietoliikennevalvonnan keskittäminen yhteen hallintokeskukseen. Ilmatieteen laitos pitää parempana vaihtoehtona muutaman verkottuneen valvontapalvelupisteen ratkaisua, joka toisi hallinnon laajuiseen toimintaan enemmän varmuutta ja redundanssia myös poikkeusoloja ajatellen sekä mahdollistaa paremmin toiminnan jatkuvan kehittymisen.

CERT-FI:n toiminnan laajentaminen asiantuntijapalveluiden kehittämiseksi tietoturvauhkien ennakointiin ja informointiin nähdään positiivisena hankkeena.

Tietoturvaan liittyvien voimavarojen keskittämisestä palveluyksiköihin oli tehty hyvin alustavia voimavaralaskelmia. Samanaikaisesti pitää tarkastella laajemmin keskittämisen aiheuttamia vaikutuksia organisaation toimintaan. Tulee varmistaa, että kohdeorganisaatioon jää riittävästi tietoa tietoturvallisuuskulttuurin kehittämiseen. Lisäksi tulee muistaa, että viranomaisilla on velvoitteita, joita ei voi siirtää toiselle osapuolelle, kuten raportissa myös todettiin.

Lisäksi Ilmatieteen laitos huomautti, että raporttiluonnoksesta puuttui ympärivuorokautisten toimijoiden joukosta kokonaan sen oma operatiivinen toiminta. Ilmatieteen laitoksen toiminnan esittely lisättiin esimerkkien joukkoon.

6 Keskusrikospoliisi

Keskusrikospoliisi toteaa lausunnossaan seuraavaa.

Työryhmä ehdottaa, että menossa olevan palvelukeskushankkeen osana parannetaan myös valtionhallinnon ympärivuorokautista tietoturvapäivystystä. Ympärivuorokautinen tietoteknisten uhkien koordinoinnin ja tietoliikennetekniikan tietoturva-asiantuntijuus tulee työryhmän mielestä perustaa viestintävirastoon kehittämällä olemassa olevia toimintoja. Tietoverkkojen ja -järjestelmien turvaamiseen liittyvät ympärivuorokautiset käyttö- ja valvontatoiminnot tulee työryhmän mielestä sisällyttää Rovaniemellä toimivan Poliisin tietohallintokeskuksen palvelutarjontaan laajentamalla asiakaskuntaa nykyisistä turvallisuusviranomaisista laajemmalle valtionhallintoon.

Työryhmän esitys ympärivuorokautisen tietoturvatoiminnan sijoittamisesta olemassa olevien yksiköiden yhteyteen on oikeansuuntainen. Virastot ovat viime kädessä itse vastuussa tietoturvastaan, mutta ympärivuorokautisen-tietoturvapalvelun järjestäminen jokaiseen organisaatioon erikseen on kallis ratkaisu. Poliisin tietohallintokeskukselle kaavailtu rooli ja asiakaskunnan laajentaminen koko valtionhallintoon voi olla perusteltua, mutta siinä yhteydessä on turvattava vähintään nykyinen PTHK:n palvelutaso poliisihallinnolle. Poliisin tietoturva ja tietohallinto eivät saa kärsiä toimialueen laajenemisesta.

7 Kauppa- ja teollisuusministeriö

Kauppa- ja teollisuusministeriö pitää laadittua selvitysluonnosta kattavana ja hyvin valmisteltuna. Ministeriönkin kantana on, että kaavailtua koordinoitua tietoturvatoimintaa tulee kehittää sellaisten organisaatioiden verkostoyhteistyönä, jossa osaamista jo nykyisessä muodossaan on olemassa.

Ministeriö esittää selvitysluonnosta kehitettäväksi nostamalla tarkasteluun seuraavia seikkoja:

Tietoturvapoikkeamatapauksen tiedonvälityksen ja selvitysprosessin kuvauksessa olisi hyvä käyttää apuna grafiikkaa, josta ilmenisi kaavailtujen osapuolten toimintamalli prosessin eri vaiheissa (virasto, hallinnon palvelutarjoajat, kaupalliset palvelutarjoajat, ohjausmalli, viestintä jne.).

Päivystyspalvelun aiheuttamia kustannuksia virastoille sekä niiden hallintaa on käsitelty esityksessä melkoisen yleisluontoisesti. Koska virastojen meno-kehykset tulevat tulevina vuosina todennäköisesti supistumaan, tulisi hyöty/kustannusproblematiikkaa avata esimerkkilaskelmin (esim. pohjautuen joihinkin tapahtuneisiin tietoturvaloukkaustilanteisiin, joiden taloudelliset vaikutukset voidaan arvioida).

Edelleen – vaikka tietoturvallisuus onkin hallinnon sähköisessä toiminta-mallissa keskeinen tekijä – tarkastelussa tulee korostetummin huomioida eri virastojen ja laitosten erilaiset toimintakentät sekä niistä johtuvat erilaiset tarpeet tietoturvan tavoitetason suh-

teen. Siirryttäessä ohi perusjärjestelmien hallinnon ydintoimintaan tulisi virastojen tärkeysluokituksen ohella olla luokiteltuna keskeiset tietojärjestelmät ja niiden väliset riippuvuudet.

Kaupallisten palvelutarjoajien osalta tarkastelu jää pintapuoliseksi ja esityksessä todetaankin, että asiaa tulisi tarkastella jatkotyössä. Työn tuloksena tulisi tällöin syntyä konkreettinen malli siitä, miltä osin ympärivuorokautista tietoturvatoimintaa on syytä hoitaa viranomaistyönä ja mitkä osiot ovat hankittavissa kaupallisilta palvelutoimittajilta. Valtion omien tietohallintoresurssien merkittävä uudelleenkohdentaminen tietoturvatehtäviin on lyhyellä aikavälillä haasteellista vaikka eläköityminenkin huomioitaisiin osatekijänä.

Luonnoksen kieliasua tulisi jonkin verran parantaa tautologian ja puhekielisten ilmaisujen poistamiseksi.

8 Poliisin tietohallintokeskus

Poliisin tietohallintokeskus toteaa, että sen toimintaa on mahdollista kehittää tämän raportin hengen mukaisesti esimerkiksi ValtIT-hankkeeseen liittyvänä tuottavuushankkeena nykyistä laajemmin Sisäasiainministeriötä palvelevaksi ympärivuorokautista tietoturvapalvelua tarjoavaksi virastoksi. Tätä kehitysmahdollisuutta harkittaessa tulee kuitenkin taata, että poliisin tietohallintopalvelut vastaavat kaikissa olosuhteissa poliisitoiminnan tarpeita.

9 Pääesikunta

Pääesikunnan lausunnossa todetaan, että valtionhallinnolta tulee edellyttää jokahetkistä kykyä torjua tietoturvauhkia. Järjestelmien tietoturvaa tulee tarkastella osana laajaa valtionhallinnon kokonaisuutta. Tarkastelemalla yksittäisten järjestelmien tietoturvaa osana valtionhallinnon tietoturvallisuuden kokonaisarkkitehtuuria, voidaan luoda kattavaa tietoturvaa sekä tunnistaa kokonaisjärjestelmän riskit ja hallita niitä.

Keskittämällä tietoturvatoiminta valtinhallinnossa voidaan tehokkaammin hallita tätä kokonaisuutta etenkin, kun hallinnonaloilla käytössä olevat laitteet, järjestelmät ja ohjelmistot ovat monilta osin hyvin samanlaisia. Valtionhallinnon organisaatioiden toiminta ja tietoturvallisuuden tarpeet ovat hyvin erilaisia ja siksi myös tietoturvatoiminnan kokonaisuus muodostuu hyvin erilaisista osista. Nämä osat on suunniteltava osana kokonaisuutta kattavan tietoturvallisuuden saavuttamiseksi. Keskittämistä suunniteltaessa on huomioitava, että monet tapahtumat edellyttävät edelleen järjestelmätoimittajan toimenpiteitä, kuten esimerkiksi tietojärjestelmän hätäpysäytys.

Ympärivuorokautinen asiantuntijuus on luonteeltaan ei-reaaliaikaista eikä se edellytä pääsyä kohdeviraston verkkoon. Tällaisenaan toiminto on helppo järjestää, koska se ei tarvitse teknisiä erityisjärjestelyitä. Nämä palvelut voidaan keskittää virtuaalisesti yhteen

päivystysryhmään, joka fyysisesti toimii hajautettuna eri organisaatioissa.

Ympärivuorokautinen operatiivinen tietoturvatoiminta saattaa olla hyvinkin reaaliaikaista ja edellyttää ylläpitotoimia järjestelmäomistajien organisaatiossa. Näiltä osin toiminta on nykyjärjestelmin hyvin vaikea keskittää. Keskitetyn päivystysorganisaation lisäksi tarvitaan päivystysryhmiä myös hajautetusti ero palvelukeskuksissa. Mikäli kohdeorganisaation toiminta on luokitukseltaan ja ylläpitotarpeiltaan matalaksi luokiteltu, saattaa keskitetty 24/7-päivystys myös operatiivisen toiminnan osalta olla riittävä.

Ympärivuorokautinen valvonta on hälytyspalvelun, analysoinnin, heikkouksien etsinnän ja testaamisen osalta järjestettävissä keskitetysti. Varsinainen järjestelmien reaaliaikainen valvonta keskitetysti edellyttää kuitenkin järjestelmäkehitystä ja onnistuakseen kattavasti sen on pohjauduttava valtionhallinnon tietojärjestelmien kokonaisarkkitehtuurin tuntemukseen.

CERT-FI -ryhmän ja virastojen välisen ei-julkisen tiedonvaihdon tarpeisiin on valvontaan liittyen kehitettävä media ja ohjeistettava toimintatapa, jolla tiedonvaihto tapahtuu. Tulevaisuudessa luontevan alustan tällaisen media toiminnalle muodostaa secnet-palveluympäristö, joka jo alkuvaiheessaan kattaa ainakin turvallisuusviranomaisten toimintaympäristön. Myöhemmissä vaiheissa ympäristöä voidaan levittää hallitusti tietoturvatoiminnan tarpeisiin laajemmallekin valtionhallintoon.

Palvelukeskukset, resursointi ja ulkoistaminen

Tulevaisuudessa valtionhallinnon yhteisiä tietojärjestelmäpalveluita tarjotaan palvelukeskuksista, joita muodostetaan eri hallinnonaloille. Tällaisessa palvelukeskusympäristössä luontevin toimintaympäristö tietoturvallisuuden palvelukeskukselle on secnet-palveluympäristö, joka kattaa turvallisuusviranomaiset ja täten kaikkein keskeisimmät tietoturvallisuustoiminnan tarvitsijat. Tietoturvallisuustoiminta voidaan pilotoida secnet-ympäristössä ja laajentaa palvelumallia myöhemmin laajemmalle valtionhallintoon ydintoimintojen säilyessä secnet-verkossa.

Itse palvelukeskus voidaan hajauttaa secnet-ympäristössä esimerkiksi kolmeen fyysiseen keskukseen, joiden toiminnot voidaan suunnata erikoistumaan mainitun kolmijaon pohjalle – ympärivuorokautinen asiantuntijuus, ympärivuorokautinen operatiivinen toiminta ja ympärivuorokautinen valvonta. Secnet-työn aikataulu sopii selvitysluonnoksessa esitettyyn aikatauluun.

Mikäli tietoturvapalvelun suunnittelua varten perustetaan erillinen työryhmä, sen tulisi toimia kiinteässä yhteistyössä secnet-työryhmän kanssa. Jos pilotointiympäristönä käytetään secnet-ympäristöä, työryhmä saattaa olla edullista perustaa jopa secnet-johtoryhmän alaisuuteen.

Resursoinnista on todettava, että jos keskitetyn palvelun järjestämisellä saavutetaan toiminnan tehostumista, niin vapautuvat resurssit on kohdennettava tietoturvallisuuden kehittämiseen uusia uhkia vastaavasti.

Selvitysluonnoksessa mainittu 80% säästön saavuttaminen joissain osatoiminnoissa tuntuu epärealistiselta ainakin, jos puhutaan merkittävistä toiminnoista. Noin suuren säästön mainitseminen saattaa aiheuttaa sekaannusta ja epärealistisia odotuksia tietoturvatoimintojen keskittämisellä saavutettaviin säästöihin.

Työryhmä jättää raportissaan varsinaisen euromääräisen kulurakenteen ja henkilölukumäärien tarkemman laskennan jatkotyössä tehtäväksi. Kulurakenteen määrittämisen ongelmaksi saattaa muodostua, etteivät varsinaiset tietoturvallisuuteen käytetyt kulut ole helposti eroteltavissa vertailun tekemiseksi. Vastaava ongelma on kohdattu jo tietohallinnon kulujen määrittelyssä.

Teknisten palveluiden ulkoistettavien osien määrittely edellyttää valtionhallinnon kokonaisuuden tietojärjestelmäarkkitehtuurin huomiointia, muuten ulkoistus saattaa vaarantaa kokonaisuuden tietoturvallisuuden. Ostettavat palvelut on kuvattava palvelusopimuksissa yksityiskohtaisesti palvelutasovaateet ja myös kriisiajan toiminta huomioiden.

Valtionhallinnon ympärivuorokautisen tietoturvatoiminnan kehittämisen ratkaisuja

Puolustusvoimien näkökulmasta valtionhallinnon ympärivuorokautisen tietoturvatoiminnan kehittäminen ja sen ydintoimintojen toteuttaminen tulisi tapahtua secnet-palveluympäristössä. Secnet voi toimia pilotointiympäristönä, josta palveluita voidaan sitten laajentaa muualle valtionhallintoon. Ratkaisua puoltaa myös se, että tämän hetkisillä viranomaisten 24/7-periaatteilla toimivilla tietoturvatoimijoilla tulee joka tapauksessa olemaan tiivis kytkentä secnet-ympäristöön. ”Tietoturvapalvelukeskus” on jaettavissa kolmeen fyysiseen keskukseen, jotka voivat erikoistua edellä esitetyllä tavalla.

Valtionhallinnon muita palvelukeskuksia kehitettäessä on tukena oltava kokonaisuutta koskeva tietoturvakonsepti, joka takaa eritasoisten palasten liittymisen aukottomasti tietoturvallisuuden kokonaisuuteen. Tietoturvallisuuden paras asiantuntemus organisoitaisiin ”tietoturvapalvelukeskukseen”, mutta muille palvelukeskuksille jäisi edelleen vastuuta erityisesti operointiin liittyvän tietoturvallisuuden ylläpidossa ja uhkilta suojautumisen toimenpiteissä.

10 Liikenne- ja viestintäministeriö

Liikenne- ja viestintäministeriö pitää valtionhallinnon tietoturvatoiminnan kehittämistä välttämättömänä ja erittäin tärkeänä kehittämisalueena. Valtionhallinnon järjestelmäpalvelut ovat toiminnassa ympärivuorokautisesti, minkä pitäisi luonnollisesti näkyä myös tietoturvan hallinnassa ja organisoinnissa. Riskien lisääntyminen ja ongelmien leviämisen nopeus tekevät ympärivuorokautisista palveluista välttämättömiä ja ne tulisi myös organisoida suunnitelmallisesti.

Raportissa korostetaan, että CERT-FI:n kanssa päällekkäisiä toimintoja ei tulisi rakentaa. Tästä lähtökohdasta tulisi liikenne- ja viestintäministeriön näkemyksen mukaan pitää ehdottomasti kiinni myös jatkossa. CERT-FI:llä on vakiintuneet toimintatavat ja sen asema Suomen johtavana ja virallisena tietoturvallisuusuhkien asiantuntijaryhmänä on laajasti tunnustettu. CERT-FI:n toimintaa kehitetään jatkuvasti, ja sen rahoituksen kehittämismahdollisuuksia ja resurssien lisäämismahdollisuuksia pyritään selvittämään.

Päällekkäisten toimintojen sijasta tulisi pyrkiä jatkossa kehittämään CERT-FI:n ja muiden valtionhallinnon toimijoiden yhteistyötä siten, että yhteistyö sujuisi entistä paremmin ja CERT-FI pystyisi entistäkin paremmin palvelemaan myös valtionhallintoa. Erityisen tärkeää olisi kehittää tiedonkulkua valtionhallinnosta CERT-FI:hin päin, mikä ei ole tähän asti toiminut tyydyttävällä tavalla.

Viestintävirastossa on jatkuvasti kehitetty myös tilannekuvatoimintaa eri toimijoiden tarpeita vastaavaksi. Lausunnon kohteena olevassa selvitysluonnoksessa on viitattu valtionhallinnossa kehitettävään uhkakuvien visualisointihankkeeseen, mikä on eräänlainen valtionhallinnon tarpeisiin keskittyvä tilannekuvahanke. Myöskään tältä osin ei liikenne- ja viestintäministeriön käsityksen mukaan tulisi kehittää valtionhallintoon erillisiä päällekkäisiä toimintoja, siinä määrin kuin CERT-FI:n tilannekuva kykenee yhteistyötä kehittämällä täyttämään valtionhallinnon tarpeet.

Liikenne- ja viestintäministeriön näkemyksen mukaan jatkossa olisi hyvä pohtia ympärivuorokautisen valvonnan ja operoinnin lisäksi myös sitä, missä määrin valtionhallinnossa voitaisiin kehittää yhteisiä ratkaisuja, joilla tietoturvan valvonta ja torjunta voidaan ainakin jossain määrin automatisoida. Ratkaisujen tulisi olla joko jaettuja tai monistettavia.

Liikenne- ja viestintäministeriö haluaa kiinnittää huomiota myös siihen raportissa esiin tuotuun seikkaan, että jos valtionhallinnon tietoturvan päivystyskeskuksia on ainoastaan yksi, tilanne saattaa olla poikkeusoloihin varautumisen osalta haastavampi kuin jos päivystyspisteitä olisi useita. Tähän seikkaan tulisi kiinnittää jatkoarvioinnissa huomiota.

Selvitysluonnoksessa ei ole kovin paljon pohdittu sitä, että suuri osa valtionhallinnon keskeisistä järjestelmistä toimii ulkopuolisten palveluntarjoajien ylläpitäminä ja tämän kautta integroituvat myös palveluntarjoajien tietoturvapalveluihin. Jatkossa olisi hyvä pohtia myös tähän liittyviä ongelmia ja toimintamalleja. Tietoturvavalvonnan ja ylläpidon eriyttäminen muusta ylläpidosta ja palveluinfrastruktuurista voi olla joltain osin erittäin haasteellista.

11 Rahoitustarkastus

Rahoitustarkastus pitää kannatettavana, että myös valtionhallinnossa tietoturvan tasoa nostetaan järjestämällä tietoturvatilanteisiin ympärivuorokautisesti reagoiva palvelu.

Rahoitustarkastuksella ei ole huomautettavaa selvitysluonnoksessa esitettyyn kahteen keskittämisehdotukseen, eli että

- ympärivuorokautinen tietoteknisten uhkien koordinoinnin ja tietoliikennetekniikan tietoturva-asiantuntijuus tulisi perustaa Viestintävirastoon CERT-FI-toiminnan olemassa olevia toimintoja kehittämällä, ja että
- tietoverkkojen ja -järjestelmien turvaamiseen liittyviä ympärivuorokautisia käyttö- ja valvontapalvelutoimintoja tulisi sisällyttää Rovaniemellä toimivan Poliisin tietohallintokeskuksen palvelutarjontaan laajentamalla asiakaskuntaa nykyistä laajemmalle.

Rahoitustarkastus kannattaa myös pienempien yksiköiden tarpeisiin vastaamista keskittämällä näiden tietoturva-asiantuntemuksen voimavaroja jo olemassa oleviin tukiorganisaation osiin.

Rahoitustarkastus ei ota kantaa ehdotusten (budjetti) taloudellisiin edellytyksiin vaan pelkästään niiden toiminnallisuuteen.

12 Sisäasiainministeriö

Sisäasiainministeriö esittää lausuntonaan seuraavaa.

Lausuntopyynnön kohteena olevassa selvityksessä on kuvattu ympärivuorokautisten tietoturvapalveluiden tarvetta, nykyistä palvelutarjontaa, vaihtoehtoisia tai toisiaan täydentäviä toteuttamisvaihtoehtoja sekä tehty ehdotus mainitun palvelun toteuttamiseksi. Selvityksen laadintaan on osallistunut merkittävällä panoksella myös SM:n hallinnonalan edustajia.

Sisäasiainministeriö pitää tarpeellisena ympärivuorokautisen tietoturvatoiminnan ulottamista koskemaan kaikkia merkittäviä valtionhallinnon organisaatioita ja toimijoita. Sisäasiainministeriöllä on omakohtaisia kokemuksia toiminnan tärkeydestä sekä myös osasta selvityksessä ehdotetuista toimintamalleista. Sisäasiainministeriöllä ja ehdotuksessa mainitulla Poliisin tietohallintokeskuksella (PTHK) on palvelusopimus, jonka mukaan PTHK tuottaa mm. kuvatuntyyppisiä tietoturvapalveluita monien SM:n hallinnonalan yhteisten tietotekniikka- ja tietoliikennepalveluiden osalta hallinnonalamme käyttäjille. Kokemuksemme mainitun keskitetyn palvelun osalta ovat olleet myönteisiä.

Selvityksen keskeisimpinä kohtina voidaan pitää tietoturvapalvelun toteuttamista osana valtion palvelukeskuksen tarjontaa käsittelevää lukua 5 (ValtIT-hankkeeseen kuuluva asia) sekä raportin lopun luvun 9 ratkaisuehdotuksia. Ehdotuksessa on käytetty kuitenkin monin paikoin melko ehdottomia termejä ”tulee”, ”on sisällytettävä” jne. Näitä tulisi välttää, koska tarvittavan palvelun rakentamisessa on käytettävissä useampiakin erilaisia ratkaisumalleja ja niissä tulee ottaa huomioon myös kaupallisten toimijoiden tarjoamat mahdollisuudet.

Sisäasiainministeriö pitää tärkeänä, että nyt selvityksen ja siitä saatavien lausuntojen pohjalta käynnistetään valtion ympärivuorokautisten tietoturvapalveluiden toteuttamis-

hanke. Se ei voi enää ole jatkossa vain VAHTI-tietoturvallisuusryhmälle kuuluva asia, vaan palvelun organisointi tulisi nyt antaa ValtIT-hankkeelle ja kytkeä se meneillään olevan Valtion IT-palvelut- osahankkeen yhteyteen ja toteutettavaksi sen tulevien ehdotusten mukaisesti ja yhteydessä.

Jatkotyössä on vielä tarkemmin selvitettävä, mikä tarjottavasta yhteisestä palvelussa tuotetaan esimerkiksi viranomaisten toimesta ja missä määrin niiden tuottamisessa on tarpeen tai syytä käyttää myös kaupallisten atk-toimittajien palveluita. Myös toiminnan rahoitukseen tai palvelumaksuihin liittyvät asiat on ratkaistava.

Selvityksessä mainittujen mahdollisten viranomaistoimijoiden (Viestintävirasto; CERT-FI ja Poliisin tietohallintokeskus) osalta sisäasiainministeriö toteaa, että kummallakin organisaatiolla voi olla oma roolinsa jatkossa palveluiden tuottamisessa. Poliisin tietohallintokeskuksen roolin osalta asioista on kuitenkin sovittava sisäasiainministeriön poliisiosaston sekä Poliisin tietohallintokeskuksen kanssa. Lähtökohtana on kuitenkin se, että PTHK:n mahdollisen palvelutoiminnan ja sen edellyttämän resurssoinnin tai muiden investointien kulut on pystyttävä korvaamaan täysimääräisesti PTHK:lle eli palvelua voidaan tuottaa ainoastaan ns. nettobudjetointimallin puitteissa.

13 Sosiaali- ja terveysministeriö

Sosiaali- ja terveysministeriö toteaa selvityksen käsittelevän asioita, jotka ovat STM:ssä hyvin ajankohtaisia. STM:llä ei ole huomauttamista selvityksen suhteen.

14 Suojelupoliisi

Suojelupoliisi esittää lausuntonaan seuraavaa.

Selvitys poikkeaa sisällöltään ja käsittelytavaltaan suhteessa siihen neutraaliin linjaan, jota VAHTI ohjeineen edustaa.

Selvityksen mukaan virka-ajan ulkopuolelle sattuvat tietoturvapoikkeamat tai välttämättömät korjauspäivitykset aiheuttavat merkittäviä vaikeuksia hallinnolle. Valtionhallinnolla ei ole tällä hetkellä kattavaa yhdenmukaista ympärivuorokautista tietoturvatilanteisiin reagoivaa palvelua.

Selvityksen mukaan ympärivuorokautinen tietoturvauhkien koordinoinnin ja tietoliikennetekniikan asiantuntijuus tulee perustaa viestintävirastoon CERT-FI-toimintaa kehittämällä. Tietoverkkojen ja järjestelmien turvaamiseen liittyviä käyttö- ja valvontapalveluja tulisi sisällyttää Rovaniemellä toimivan Poliisin tietohallintokeskuksen palvelutarjontaan laajentamalla sen asiakaskuntaa nykyisistä turvallisuusviranomaisista laajemmalle valtionhallintoon.

CERT-FI:n osalta ehdotettu nykyisten toimintojen kehittäminen ja laajentaminen on lähtökohdiltaan realistinen. Yksikkö on rakentanut toimivan yhteistyöverkoston, johon sisältyy paitsi valtion turvallisuus- ja tietointensiivisten toimielimien edustajia myös yksityisen sektorin tietoturva-alan toimijoita. Tietojärjestelmäriippuvuuden kasvaessa on tosin tarvetta lisätä tietoturvaresursseja myös muissa valtionhallinnon yksiköissä mukaan lukien CERT-FI:n yhteistyötahot. Tämän tulee luonnollisesti tapahtua yleisten voimavarojen sallimissa puitteissa.

Poliisin tietohallintokeskuksen roolia koskeva osuus on ongelmallisempi. Poliisin tietohallintokeskus on perustettu lähtökohtaisesti poliisihallinnon tietojärjestelmäpalveluita hoitavaksi virastoksi. Se hoitaa myös mm. sisäasiainhallinnon tietoliikenneverkon operointiin liittyviä tehtäviä.

Ehdotettu tehtävien lisäys merkitsisi tarvetta lisähenkilöstörekrytointiin Poliisin tietohallintokeskukseen. Palvelun tuottamisen kannalta Rovaniemen fyysinen sijainti asiakkaiden suhteen saattaisi aiheuttaa käytännön ongelmia, sillä huolimatta kehittyneistä tietoliikenneverkoista ja etähallintaratkaisuista monet järjestelmät vaativat nyt ja jatkossakin usein asiantuntijan fyysistä läsnäoloa. Palvelun tuottamiseen liittyvä hallinnointi kehittämispalavereineen ei myöskään toimi käytännössä kaikilta osin etätyönä, mistä on osoituksena jo tämänhetkiset Poliisin tietohallintokeskuksen huomattavat matkustusmenot. Myöskään tietoliikenteellisesti Rovaniemen sijainti ei ole täysin ongelmaton suhteessa sen potentiaalisiin uusiin mahdollisiin asiakkaisiin.

Koska virastot eivät toimi 24H -periaatteella, aiheuttavat yllättävät tietoturvapoikkeamat väistämättä ongelmia. Toistaiseksi virastot ovat pystyneet varsin hyvin näistä selviytymään mm. työaikajoustoja hyödyntämällä.

Selvityksessä hahmoteltu hallintamalli tarkoittaisi käytännössä useiden virastojen keskeisten tietojärjestelmien pääkäyttäjäoikeuksien luovuttamista viraston ulkopuoliselle taholle.

Palvelun käyttäjän näkökulmasta vaihtoehtoisten palvelujen tarjonnan vaihtoehdot olisi syytä pitää mahdollisena joko pitämällä palvelu viraston sisäisenä toimintona, luomalla valtionhallintoon useampia vaihtoehtoisia palveluntuottajia tai mahdollistamalla yksityisen palveluntarjoajan vaihtoehdon käyttäminen ja aito kilpailutilanne.

15 Tekninen korkeakoulu

Tekninen korkeakoulu esitti laajasti parannuksia luettavuuteen ja kieliasuun. Näitä kommentteja otettiin parhaimman mukaan huomioon raporttia viimeistellessä.

Tekninen korkeakoulu tähdentää kriittinen tietoturvapalvelun toteuttamisesta seuraavaa. Johdannossa todetaan, että kriittinen tietoturvapalvelu voi olla yhteen palveluntarjontaorganisaation keskitetty tai se voi muodostua usean palveluntarjoajan yhdessä muodostamasta päivystyspalvelusta. Vaikkakin kriittisen tietoturvapalvelun saattaisi voida

keskittää yhteen palveluorganisaatioon, niin on syytä korostaa, että siinä tapauksessa palveluorganisaation on oltava valtion oma virasto tai laitos. Koko valtionhallinnon kriittistä tietoturvapalvelua ei voi rakentaa yhden kaupallisen toimittajan varaan. Valtionhallinnon sisälläkin yksi fyysinen toimipiste, jonka tuhoamalla tuhottaisiin koko valtion kriittinen tietoturvapalvelu, kuulostaa riskaabelilta. Vastuuorganisaatioita voi toki olla yksi.

Johdon tiivistelmässä todetaan, että uhkien koordinointi ja tietoliikenteen tietoturva-asiantuntijuus toteutettaisiin CERT-FI -toimintaa kehittämällä. Toisaalta taas verkkojen ja järjestelmien turvaamisen operatiivinen toiminta esitetään tapahtuvaksi PTHK:ssa Rovaniemellä. Uhkakoordinoinnissa on TKK:n mukaan aivan riittävästi työtä sellaisenaan, ja CERT-FI:n pitäisi pyrkiä tekemään siitä hyvä palvelu. Tietoliikenteen tietoturva-asiantuntijuutta ei ole järkeä erottaa operatiivisesta toiminnasta, koska tietoliikenne on myös siinä nykyisin aivan olennaisessa osassa.

Harva palvelin- tai palveluylläpitäjä ymmärtää tietoliikenteestä niin paljon kuin olisi suotavaa, eikä tätä tilannetta pidä nykyisestään ainakaan aktiivisesti huonontaa erottamalla tietoliikenteen asiantuntijoita, erikoistuneita tietoturvaan tai ei, organisaatioon, joka ei ole vastuussa operatiivisesta toiminnasta. Parasta olisi, jos operatiivisen toiminnan organisaation tietoliikenneasiantuntijoiden osaamista kartutettaisiin niin, että heidän pitää ymmärtää myös tietoliikenteen tietoturvaa syvällisesti.

TKK analysoi ympärivuorokautisen tietoturvapalvelun toteuttamisaikataulua seuraavasti. Kysymys on niin laajasta asiasta, että sen valmisteluun kuluu päätoimisesti asiaa toteuttavalla ryhmällä luultavasti vuoden verran. Palvelua ei myöskään missään tapauksessa pidä ottaa käyttöön ilman kenttätestausta, jossa mahdolliset viat ja virheet etsitään ja korjataan. Siihen voi kulua jälleen yksi vuosi. Vasta tämän jälkeen voidaan ajatella palvelun ottamista käyttöön.

Käyttöönotostakin olisi tarpeen tietää, onko se valinnaista vai pakollista, jotta kaikki osapuolet pystyvät varautumaan tapahtumaan. Aikataulutus tulee valmistella paljon huolellisemmin ja perustella esitetyt arviot.

16 Tilastokeskus

Tilastokeskus toteaa lausunnossaan, että ympärivuorokautisia keskitettyjä tietoturvapalveluja tarvitaan, koska yksittäiset virastot eivät voi tuottaa niitä kustannustehokkaasti itse. Uusiin palveluihin liittyy toimivalta kysymyksiä. On siis tärkeää, että palvelun tarjoajien roolit ovat selkeät, toiminnoissa vähän päällekkäisyyksiä ja että asiakas voi luottaa saavansa sitä palvelua mitä tarvitsee.

Tilastokeskus on useassa yhteydessä korostanut, että tietohallinto palveluja tuotettaessa on tärkeää, että keskitettyjä lähdetään rakentamaan selkeästi todetun tarpeen pohjalta. Palveluun liittyminen ei saa vaatia etukäteissitoutumista, palvelutason on oltava houkutteleva ja hinnan niin kilpailukykyinen, että siihen liittyminen on luontevaa ja että se

on toiminnallisesti ja taloudellisesti varteenotettava vaihtoehto omalle palvelulle tai palvelun ostamiselle muulta tarjoajalta.

Keskittäminen tuo selvityksen mukaan lisäarvoa 24/7 palvelun laite- ja ohjelmistohankintojen ja erityisosaamisen muodossa. Se ei kuitenkaan merkitse välttämättä, että virasto voisi vastaavasti luopua näihin palveluihin käyttämistään resursseista, vaan vapautuville resursseille löytyy nopeasti vaihtoehtoiskäyttö. Tästä syystä keskittäminen ei välttämättä tuo säästöjä ainakaan lyhyellä tähtäyksellä. Esitetyt laskelmat keskitetyn palvelun edullisuudesta ovat sikäli keinotekoisia, että jos virastot eivät pysy ympärivuorokautisia palveluja itse järjestämään, ei sen varan kannata myöskään vertailua perustaa.

Raportissa ei ole juurikaan esitetty millaisia riskejä keskittämiseen mahdollisesti liittyy.

Tieto- ja viestintäverkkojen uhkien visualisointi ja mallintaminen esitetään tietoturvapalvelun eräänä haasteena. Miten tutkimukseen vahvasti viittaava tehtävä olisi sovitettavissa palvelukeskuksen toimintaan jää arveluttamaan. Eikö tämä kuuluisi yliopistojen ja korkeakoulujen rooliin, vaikka siihen olisi käytettävissä myös palvelukeskuksen erityisosaamista ja resursseja.

Tilastokeskus päättää lausuntonsa todeten, että uusia 24/7 palveluja eittämättä tarvitaan julkishallinnossa. Palveluja tulisi olla yleisesti käytettävissä hallinnonrajoista tai viraston koosta riippumatta. Ovatko ne toteutettavissa nykyisten organisaatioiden puitteissa vai yhden tai useamman palelukeskuksen palveluna vaatii vielä lisäpohdintaa. Lähtökohtia tähän selvitys antaa, mutta päätöksen tekoa varten esitysten on vielä tarkennuttava.

17 Valtiokonttori

Valtiokonttorin lausunnossa todetaan seuraavaa.

Kuten työryhmä on todennut, kaikilla virastoilla ja laitoksilla ei ole asiantuntemusta eikä resursseja niitä hankkia tietoturvan kehittämiseksi ja ylläpitämiseksi. Kaikilla virastoilla on kuitenkin tarve turvata viraston hallussa olevat tiedot ja niiden käsittely. Vastuu tietoturvasta on virastolla.

Tietoturvavaatimusten ja turvan taso vaihtelee virastoittain. Kaikilla on kuitenkin tarve saada tietoja mahdollisista tietoturvauhkista ja muista toiminnan jatkuvuutta häiritsevistä tekijöistä. Virastojen kohdalla tämä tarkoittaa asiantuntijapäivystyksen järjestämistä siten, että vakaviin uhkiin reagoiminen voidaan välittömästi käynnistää virastotasolla.

Ympärivuorokautisen tietoturvatoiminnan tarve kasvaa sähköisen asioinnin palveluiden lisääntyessä sekä palvelukeskusten perustamisen ja alueellistamisen sekä keskitettyjen tietojärjestelmien käyttöönoton myötä.

Valtion ympärivuorokautisen tietoturvatoiminnan järjestäminen valtionhallinnon yhteisenä palveluna on perusteltua mm. suuremman yksikkökoon tuomana kustannustehokkuutena ja korkeatasoisen osaamisen ylläpitämiseksi. Tällöin on kuitenkin tarkkaan harkittava palvelun tuottamisen muoto, vaihtoehtoina itse tuotettu palvelu, ostettu palvelu tai

näiden yhdistelmä. Muistiossa esitetty palveluryhmittely asiantuntija-, operatiiviset ja valvontapalvelut tasoille on hyvä lähtökohta arvioida vaihtoehtoisia tapoja tuottaa palvelu. Muistiossa esitetty peruste palvelun tuottamiseksi omin resurssein, toimiminen virkavastuulla, kannattaisi perusteena vielä arvioida uudelleen. Lisäksi on syytä arvioida valtionhallinnon mahdollisuudet ylläpitää korkeatasoista osaamista ja työnantajakilpailukykyä tällä tehtäväalueella yksinomaan omin henkilöresurssein.

Tehokkaan toiminnan varmistamiseksi valtionhallinnon perustietotekniikan yhtenäistäminen ja palvelutuotannon keskittäminen on tärkeää. Tällöin myös tietoturvallisuuden toteutuminen on järjestettävissä kustannustehokkaammin keskittämällä tietoturvapalveluiden tuottamista. Tämä vahvistaisi valtionhallinnon toimintaedellytyksiä sekä normaali- että poikkeusoloissa.

Keskitettyjä tietoturvatoimintoja luotaessa on kuitenkin huomioitava, että virastojen tietoverkkojen ja tietojärjestelmien omaa valvontaa ratkaisu ei poistaisi ennen kuin keskitetty tietoturvatoiminto on voitu kytkeä keskitetysti tuotettuihin palveluihin.

Valtiokonttorin mielipiteen mukaan keskitettyjen tietoturvapalveluiden tuotanto voisi tapahtua samoin periaattein kuin perustettavana olevien talous- ja henkilöstöhallinnon palvelukeskusten toiminta, jatkossa kytkettynä valtion yhteisten IT- palveluiden tuotantoon. Palvelun tulisi perustua palvelusopimukseen jossa sovitaan sekä palvelun laatutasosta että palvelun hinnasta. Palvelun hinnoittelussa tulisi huomioida palvelun tuottamisesta aiheutuvat kokonaiskustannukset.

18 Valtion työmarkkinalaitos

Valtiovarainministeriön henkilöstöosaston valtion työmarkkinalaitos toteaa lausunnossaan toimivansa valtiovarainministeriön, valtion työmarkkinalaitoksen tai valtioneuvoston tietopalveluyksikön asiakasyritysten kanssa tekemien erillisten organisaatio- ja sovelluskohtaisten tietoturvasopimusten mukaisesti. Normaalisti virka-aikainen päivystys on riittänyt. Poikkeuksena on ollut virka- ja työehtosopimusneuvottelujen aika, jolloin ollaan henkilörekistereiden ja tiettyjen työmarkkinalaitoksen käytössä olevien sovellusten, mm. Helmi-Info -järjestelmän osalta siirrytty ympärivuorokautiseen varmistukseen järjestelmien toimivuuden osalta.

Vuoden 2006 alusta valtion työmarkkinalaitos käynnisti siirtymävaiheen uuteen valtion työmarkkinalaitoksen, ministeriöiden sekä virastojen ja laitosten henkilötietojen tarpeeseen kehitettyyn ’Työnantajan henkilöstötieto TAHTI’ -järjestelmään. Se palvelee työnantajavirkamiehiä sekä muita asiantuntijoita mm. tulosohjauksessa, taloushallinnossa, budjetoinnissa ja toiminnan suunnittelussa ja neuvottelutoiminnassa. Neuvottelutoiminnassa järjestelmän tulisi olla ympärivuorokautisessa toimintavalmiudessa vuoden 2007 neuvottelu- ja sopimuskierroksen käynnistyessä syyskesällä 2007.

Neuvotteluaikaiseen ympärivuorokautiseen tietoturvatoimintaan osallistuvat Tahti -järjestelmään siirtymisen jälkeen valtion työmarkkinalaitos, valtiokonttori, valtioneuvos-

ton tietopalveluyksikkö sekä järjestelmän toimittajat. Niiden toiminta yhdessä takaa ympärivuorokautisen operatiivisen toimintavarmuuden seuraavien osa-alueiden osalta.

- Yleisjohdon ja raportoinnin hyväksikäyttö
- Tahti-järjestelmän kokonaistoimivuus ja
- Tahti-järjestelmän tietokonepalvelut
- Ohjelmistojen toimivuus
- Tietoliikenteen toimivuus

19 Valtioneuvoston kanslia

Valtioneuvoston kanslia toteaa seuraavaa.

Valtionhallinnolla ei ole tällä hetkellä kattavaa ympärivuorokautista tieto-turvatilanteisiin reagoivaa palvelua. Kuten selvityksessä todetaan, tietoturvallisuuden vaalimisen perustarpeet ovat varsin samanlaisia valtion eri organisaatioilla, mikä antaa hyvät edellytykset tietoturvayhteistyöhön ja resurssien jakamiseen.

Valtioneuvoston kanslia kannattaa työryhmän esittämää kehittämismallia perustaa ympärivuorokautinen tietoteknisten uhkien koordinoinnin ja tietoliikennetekniikan tietoturva-asiantuntijuuden perustamista Viestintäviraston CERT-FI:n toimintoja kehittämällä. Myös ympärivuorokautisten käyttö- ja valvontapalvelutoimintojen sisällyttäminen Poliisin tietohallintokeskuksen palveluun on kannatettavaa: CERT-FI hoitaa asiantuntijuuden, jota tulee kehittää kaikkien tarpeisiin. PTHK hoitaa verkkojen tunkeutumisen valvontaa sekä varoitusten antamisen ja kokeilee korjausasennuspaketit.

On kuitenkin otettava huomioon, että käytännön toteutuksessa saattaa syntyä vaikeuksia. Asiantuntijuus (CERT-FI), operatiivinen toiminta ja valvonta ovat asianmukaisia tehtäviä, mutta hieman epäselväksi jää, mikä on toiminnan ydin. Miten henkilöstö saadaan päivystysrinkeihin, kuka maksaa ja kenen järjestelmiä valvotaan, vai valvotaanko vain verkkoa. Miten hallinnollinen vastuu hoidetaan? Millä perusteilla päivystäjä saa käynnistää esimerkiksi hätäpysäytyksen jonkun tietyn hallinnonalan verkossa. Näihin kysymyksiin pystytään ehkä vastaamaan ValtIT - hankkeen etenemisen myötä.

Valtioneuvoston kanslia katsoo, että vastuita pitää vielä tarkentaa ja lisäksi poikkeusolot on huomioitava ulkoisten resurssien käytössä ja koko toiminnan resursoinnissa. Jatkosuunnitelma verkkojen turvallisuuden päivystysyksiköstä tulee viedä poikkihallinnolliseen päätösvalmisteluun.

20 Valtiontalouden tarkastusvirasto

Valtiontalouden tarkastusvirasto katsoo, että 24h/7 vrk tietoturvapalveluhankkeet olisi tarkoituksenmukaisinta toteuttaa osana ValtIT-hanketta, kuten selvityksessä on esitetty.

21 Valtiovarainministeriön budjettiosasto

Valtiovarainministeriön budjettiosasto esittää lausunnossaan, että selvitysluonnoksessa esiin nostetut työaikojen liikkuvuusvaatimukset ja eräät poikkeukselliset tapahtumat (sodat, luonnonkatastrofit) ovat hyvin poikkeuksellisia tapahtumia, koskettavat välittömästi varsin vaihtelevasti Suomea sekä rajattua joukkoa virkamiehiä tai viranomaisyksiköitä. Niiden perusteella voidaan perustella palvelutarpeen jatkuvaa tai yleistä käyttöä lähinnä rajallisesti.

Selvitysluonnoksen perusteella varsin harvalla valtion yksiköllä on ollut tarvetta jatkuvasti miehitettyyn 24/7 tyyppiseen tietoturvapäivystykseen. Tietoturvapäivystys ei myöskään voi koskea kaikkia valtion organisaatioiden järjestelmiä, vaan käsitys priorisoinnista täytyy olla. Voitaneen todeta, että valtaosin valtion virastojen ja laitosten perustietoturvapalvelun toteuttamiseen on riittänyt virka-aikana tapahtuva päivystyspalvelu sekä perustietoturvallisuuden ja varmistusten pitämien riittävän ajantasaisena.

Tarve 24/7-periaatteella toteutettavaan jatkuvaan tietoturvapalveluun näyttäisi rajoittuvan ensisijaisesti lähinnä nopeaa operatiivista reagointivalmiutta tarvitseviin viranomaisyksiköihin, kuten poliisiin ja puolustusvoimiin, ja niissäkin tiettyihin kriittisiksi luokiteltuihin tietojärjestelmiin.

Budjettiosaston näkemyksen mukaan selvitysluonnoksessa ei löydy selkeää vastausta sille, onko valtionhallinnossa laajempaa tarvetta ympärivuorokautiselle tietoturvapäivystykselle. Päätöksentekoa ja esitetyn erillisen työryhmän perustamista varten vaaditaan tietoa, jolla voidaan tarkemmin todentaa palvelun yleistä tarvetta hallinnossa, tarpeen laatua ja laajuutta ja rahoituspohjaa/kustannusten jakamishalukkuutta per potentiaalinen asiakasvirasto.

Automatisoinnin hyödyntäminen ympärivuorokautisessa tietoturvapalvelussa

Selvitysluonnos ei käsittele automatisoinnin hyödyntämismahdollisuuksia tietoturvapäivystyksessä, mitä voidaan pitää puutteena. Selvitysluonnoksessa esitetyn suurta virastojoukkoa ympärivuorokautisesti palvelevan miehitetyn päivystysyksikön käyttö ja ylläpito edellyttäisi paljon henkilöresursseja ja olisi kallista. Perusteita henkilöpäivystyksen tuomasta erityisestä lisäarvosta, joka perustelisi myös toiminnan suuret kustannukset, ei ole esitetty. Mm. selvityksessä esitetyt katastrofitilanteet ja vastaavat ovat hyvin poikkeuksellisia tapahtumia, joilla voidaan huonosti perustella ympärivuorokautista valvontatoimintoa.

Selvitysluonnoksen kuvaamat seuranta- ja päivystyspalvelut voidaan toteuttaa tietoliikennettä seuraavien ja analysoivien ohjelmien avulla, jotka poikkeamia havaitessaan lähettävät hälytyksen päivystysvuorossa olevalle henkilölle. Tietoturvapäivystys ei ole

kuitenkaan toimipisteeseen sidottua toimintaa. Esimerkiksi hälytyksen saatuaan päivystysvuorossa oleva henkilö voi suojatun etäyhteyden kautta tehokkaasti tutustua hälytyksen syyhyn kotona ja tämän perusteella päättää toimenpiteistä kuten palvelimen pysäyttämisestä sekä tarvittaessa hälyttää laajemman päivystysryhmän tilannetta hallinnoimaan.

Vahinkoja estäviä toimenpiteitä voidaan toteuttaa etähallinnankautta. Tietojen turmeltumista ja menettämistä voidaan estää tehokkaasti, tai vahingot ainakin minimoida, huolehtimalla tietojen riittävästä varmistuksesta. Valvonnalla ja päivystyksellä tapahtuva vahinkojen estäminen on lähinnä toissijaista.

Budjettiosasto toteaa, että selvitysluonnoksessa esitetyn toiminnon järjestämisessä automatisointia ja etä/kotityömahdollisuutta hyödyntämällä voitaisiin päästä huomattavasti kevyempään toiminto- ja kustannusrakenteeseen toiminnan varmuuden siitä kärsimättä. Valvonnan automatisoinnilla voidaan kattaa virka-ajan ulkopuolista päivystystarvetta laajasti ja tehokkaasti.

Tietoturvapalvelun tuottaminen osana palvelukeskusta

Budjettiosasto katsoo, että tietoturvapäivystyksen toteuttamisessa voidaan hyödyntää palvelukeskusrakennetta. Budjettiosaston näkemyksen mukaan useiden yksittäisten pienten samaa tehtävää tekevien toimipisteiden resurssien yhdistäminen sekä niiden palvelutoiminnan ja hankintojen keskittäminen tarjoaa säästömahdollisuuksia.

Tietoturva-asiantuntijuuden kokoaminen sekä keskitetysti toteutettava tietoturvatiedottaminen, -neuvonta ja -päivystys ovat luonteeltaan tehtäviä, jotka sopivat hyvin palvelukeskustyyppiseen organisaatioon. Samalla on mahdollista turvata ja kehittää valtionhallinnon tietoturvaosaamista sekä yhdistää eri puolilla hallintoa työskentelevien asiantuntijoiden tietämystä ja resursseja. Tällainen yksikkö pystynee tarjoamaan myös haastavan ja monipuolisen työkentän työntekijöilleen. Tämän tyyppisen toiminnan tuottamisen kontrollin säilyttämistä valtion sisällä voidaan perustella mm. työnjohdollisilla syillä.

Budjettiosaston lausunnossa myös varoitetaan, että uusia toimintoja suunniteltaessa on vaara päällekkäisistä toiminnoista. Mahdolliset resurssilisäykset olemassa oleville yksiköille eivät saa johtaa päällekkäisyyksiin mahdollisesti toteutettavan itsenäisen ympärivuorokautisen tietoturvapalveluyksikön kanssa. Budjettiosasto toteaa, että tietoturvapalvelun pystyttäminen ei saa merkitä päällekkäistä toimintaa nykyisten toimijoiden (mm. CERT-FI, PTHK) kanssa. Mikäli päädytään tietoturvatoiminnan yksikön perustamiseen palvelukeskuksen yhteyteen, tulee jatkovalmistelussa huolehtia siitä, että kyseessä ei ole päällekkäinen toiminta mm. edellä mainittujen organisaatioiden osalta.

Budjettiosasto toteaa, että jatkotyön tarpeellisuutta on vaikea arvioida, koska selvitysluonnos ei tarjoa tarkempaa tietoa palvelutarpeesta. Mikäli palvelu osoitetaan tarpeelliseksi tai toimintaa laajennetaan esim. jonkin muun yksikön puitteissa, tulee huolehtia, että ko. yksikön resurssointi voidaan toteuttaa hallituksen asettamien henkilöstön vähentämis-

tavoitteiden puitteissa. Hallitus on asettanut tavoitteeksi, että seuraavan vaalikauden loppuun mennessä valtion henkilöstömäärä vähenee vuosittain keskimäärin 2 prosentilla.

Tietoturvapalvelun toteuttamisen kustannukset

Päätöksenteon kannalta toiminnan kustannusvaikutusten riittävä esittäminen ja vaihtoehtoanalysointi ovat keskeisiä. Selvityksessä kustannustekijöitä on käsitelty puutteellisesti, mikä ei anna toiminnan kustannustasosta riittävää kuvaa.

Selvitysluonnoksessa yleistä kustannusrakennetta on kuvattu henkilöstökustannusten (palkat, sivukulut) ja koulutuskustannusten pohjalta. Selvityksessä ei esitetä yleistä kustannusrakennetta palvelutoiminnan pystyttämiseen ja tuottamiseen liittyvistä olennaisista menoeristä kuten kiinteistömenoista, atk- ja kalustokustannuksista tai puhelin-, verkko-, tietoliikenne ja tietojärjestelmäkustannuksista.

Selvitysluonnoksessa toiminnan rahoitusmallina on nähty budjettirahoitteisuus asiakasvirastojen kautta. Tarkemmin tämän mallin rahoitusmallin perusteita tai toimivuutta ei ole käsitelty.

Kustannusten tarkempi laskenta on todettu jätettävän mm. toteutushankkeelle. Kuitenkin selvitysluonnoksessa on esitetty näkemys säästöistä, kuten 50 % säästömahdollisuus henkilöstökuluista. Selvitysluonnoksessa esitetty säästöpotentiaali jää epäuskottavaksi, koska edes yleisiä arvioita perustamiskustannuksista tai sen jälkeisistä vuotuisista kustannuskertymistä ei ole esitetty. Vastaavasti myös muut toteamukset kustannushyödyistä tai kokonaiskulujen pienentämisestä pitkällä aikavälillä jäävät perustelematta ja osoittamatta.

Budjettiosasto toteaa, että selvitysluonnoksen esittämä palvelu näyttäisi merkitsevän valtiolle lähinnä uusia kustannuksia. Budjettiosaston näkemyksen mukaan selvityksestä ei löydy perusteluja näkemykselle (luku 8) ”tällaisen ryhmän henkilökulut eivät ole lisäkustannus, sillä joka tapauksessa nämä työt on jotenkin tehtävä.”

Valtionhallinnon ympärivuorokautisen tietoturvatoiminnan kehittämisen ratkaisuja

Selvitysluonnoksen laatinut työryhmä on esittänyt, että ympärivuorokautisen tietoturvatoiminnan kehittäminen ja ensimmäisen palveluratkaisun toteuttaminen liitetään tietoturvatoiminnan kannalta sopivimman hallinnon kehittämishankkeen yhteyteen valtiovarainministeriön päätöksen mukaisesti.

Budjettiosaston näkemyksen mukaan palvelukeskukseen ei kannata resursoida tai siinä kannata pilotoida palvelua, jonka käyttötarve on epäselvä tai jonka laaja hyödyntäminen rajoittuisi vain muutamaan virastoon. 24/7-tyyppiset palvelut ovat tyypillisesti sellaisia, että niiden käyttötarve vaihtelee hyvin suuresti. Vaikka valtionhallinnon tietotur-

vallisuuden kehittäminen on tärkeää ja sen ylläpitoon tulee kiinnittää huomiota, niin tarkoituksenmukaista ei ole perustaa valtiolle yksikköä ”yleistä” tietoturvallisuutta päivystämään tai valvomaan. Palvelun sisällön tulee perustua asiakastarpeeseen.

Budjettiosaston näkemyksen mukaan palvelukeskuksiin perustettavilla uusilla toiminnoilla tulee vähentää tai poistaa päällekkäistä toimintaa valtionhallinnossa. Selvitysluonnoksessa kuvatulla yksiköllä näyttää olevan päällekkäisiä tehtäviä jo olemassa olevien palveluyksiköiden kanssa ja osin myös virastojen omien tietoturvapalveluiden kanssa.

Selvitysluonnoksessa on tuotu esille useita yksittäisiä ja yleisellä tasolla kuvattuja kehittämisen ratkaisuja. Niihin tässä yhteydessä tarkemmin kantaa ottamatta budjettiosasto toteaa, että ratkaisuvaihtoehdot jäävät epäselviksi ja irrallisiksi sekä mm. vaille näkemystä toteuttamisjärjestyksestä. Selkeyden vuoksi voisi esityksiä ja ratkaisuja pyrkiä luokittelemaan ja esitystekniikkaa parantamaan.

22 Verohallitus

Verohallitus huomauttaa lausunnossaan, että virastojen ja laitosten omat edellytykset tietoturvauhkien torjuntaan tarvittavien järjestelmien ja henkilöstön hankkimiseen ovat huonot. Se pitää ehdotusta valtionhallinnon keskitetyn ympärivuorokautisen tietoturvatoiminnan järjestämisestä hyvänä ja tarpeellisen, mutta katsoo että esitetty toteutustapa vaatii vielä jatkotyöstämistä.

Verohallituksen käsityksen mukaan uhkien torjunnan koordinointi ja tietoliikennetekniikan tietoturva-asiantuntijuus on perusteltua keskittää selvitysluonnoksen mukaisesti Viestintäministeriön CERT-FI-toiminnon yhteyteen. Ympärivuorokautisen käyttö- ja valvontapalvelun sijoittamista Poliisin tietohallintokeskuksen (PTHK) yhteyteen Verohallitus pitää kuitenkin ongelmallisena.

PTHK:n varsinaisena tehtävänä on tuottaa mm. tietoturvaan liittyviä palveluja turvallisuusviranomaisille. On vaikea ajatella, että PTHK tai mikään muukaan selkeästi omia operatiivisia tehtäviä hoitava virasto pystyisi tarjoamaan tasapuolisesti palveluja myös ulkopuolisille viranomaisille. Erityisesti turvatoimintaan liittyvän käyttö- ja valvontapalvelun ulkoistaminen vaatii selkeästi kuvattuja, sanktioituja ja palvelutasoltaan määriteltyjä sopimuksia. Tällaisten sopiminen viranomaisten välillä lienee varsin ongelmallista.

Edellisestä johtuen Verohallitus pitää parempana, että käyttö- ja valvontapalvelut sijoitettaisiin joko CERT-FI-toimintoon tai johonkin muuhun soveltuvaan virastoon/laitokseen, jolla ei ole omaan toimintaan liittyvää laajamittaista tietojenkäsittelytoimintaa. Tarvittavat tietoturvatoiminnot voitaisiin sijoittaa myös ValtIT-hankkeen yhteydessä suunniteltuun IT-palveluyksikköön.

Verohallitus toteaa oletettavaksi myös sen, että yleinen mielipide pitäisi huonona ratkaisua, jossa PTHK:lla olisi näin merkittävä rooli koko valtionhallinnon tietoliikenteen turvaamisessa ja valvonnassa.

23 Viestintävirasto

Viestintäviraston toteaa lausunnossaan seuraavaa.

Internetin valtakausi on voimakas ja erilaiset tietoyhteiskunnan toimintaa uhkaavat ilmiöt ovat voimistumassa. Ilman jatkuvia ponnisteluja tietoturvan toteuttamiseksi ovat yhteiskunta ja useat sen kriittiset toiminnot haavoittuvia. Viestintävirasto pitää valtionhallinnon tietoturvatoiminnan kehittämistä välttämättömänä ja jatkuvana toimenpiteenä.

Viestintäviraston tietoturvallisuusyksikkö ja siellä toimiva CERT-FI -ryhmä on keskeinen toimija Suomen tietoturvakentässä. Tarve tietoturvatoimien jatkuvalle kehittämiselle ja riittävälle resursoinnille on myös tiedostettu virastossa, ja alue on nostettu yhdeksi tulevaisuuden painopistealueista. CERT-FI kehittää parhaillaan esimerkiksi toimintoja tietoturvallisuuden tilannekuvan muodostamiseksi siten, että etenkin ennaltaehkäisevien tietoturvatoimien osalta käytössä olisi realistinen päätöksenteon apuväline. Viestintävirasto suunnittelee lisäksi parhaillaan organisaatiotäsmennyksiä, joiden tavoitteena on vahvistaa kehittyvää tietoturva-aluetta. Viestintävirasto katsoo, että valtion ympärivuorokautisen tietoturvatoiminnan järjestämisestä tehty selvitysluonnos on lähtökohtaisesti onnistunut kuvaus nykyisistä toimista ja tulevista tarpeista kehitysehdotuksineen. Viestintävirasto haluaa kiinnittää erityistä huomiota selvityksessäkin esille nousseisiin seikkoihin kaupallisten palveluiden tarjonnan osalta sekä pienen maan rajallisiin resursseihin.

Kaupallisten palveluiden osalta selvityksen oikea havainto on niiden soveltumattomuus palvelemaan riittävän luotettavasti valtionhallinnon tarpeita kaikissa tilanteissa ympärivuorokautisesti – tämä toiminta-alue on kriittisyytensä vuoksi hoidettava viranomaisvoimin. Myös puolueettoman toimijan tärkeyttä ei voida vähätellä valtionhallinnon tietoturvatoimien toteuttamisessa. Viestintäviraston CERT-toiminto on tyyppiesimerkki puolueettomasta toimijasta, jolla on selkeät lakiin perustuvat tehtävät sekä viraston toimialan kautta laajat yhteistyökanavat keskeisimpiin tietoyhteiskunnan toimijoihin, kuten teleyrityksiin.

Pienellä maalla ei ole viranomaiskentässäkään ylimääräisiä resursseja hukattavana ja siten selvityksessä esitetyt kehittämisratkaisut ovat kannatettavia. Keskeinen vaatimus palvelun laadun ja riittävän osaamisen takaamiseksi on resurssien keskittäminen. Uusien organisaatioiden perustaminen olemassa olevien rinnalle aiheuttaisi turhaa päällekkäisyyttä sekä tarpeetonta viivettä toimien kehittämisessä. Tietoturvatoiminnan osalta on muistettava luottamuksen rakentuminen käytännön toiminnan kautta – luottamusta ei pystytä hetkessä ottamaan, vaan se ansaitaan vasta ajan saatossa.

Selvityksen nykytilan kuvaus ja eri vaihtoehtojen kartoitus on kehittämisratkaisuineen onnistunut. Selvityksessä ei kuitenkaan ole otettu kantaa kehittämistoimien vaatimiin konkreettisiin muutoksiin esimerkiksi organisaatioiden resurssien ja rahoituksen kehittämisen osalta. Tämä alue vaatinee erillisen selvitystyön. Nykyisten resurssien osalta todettakoon CERT-FI:n koostuvan neljästä teknisestä asiantuntijasta.

Lisäksi Viestintävirasto antaa lähtökohtia lainsäädännöllistä jatkotyöskentelyä varten todeten, että laki viranomaistoiminnan julkisuudesta on eräs keskeisistä aihepiiriin liittyvistä laeista. Jatkotyöskentelyssä tulisikin mahdollisuuksien mukaan laatia analyysi mahdollisista säädöstasolla olevista puutteista tai rajoituksista, jotka vaikuttavat järkevien ja tarpeellisten tietojen luovuttamiseen. Kriittisiä kohteita ovat muun muassa tunnistamistietojen ja haavoittuvuustietojen jakelu joustavasti eri organisaatioiden välillä.

Viestintäviraston täsmennys CERT-FI:n ja Viestintäviraston tietoturvallisuusyksikön henkilöstökunnan määristä huomioitiin raportissa.

24 Väestörekisterikeskus

Väestörekisterikeskus pitää tärkeänä valtion ympärivuorokautisen tietoturvatoiminnan järjestämistä ja että lausunnon pohjalta käynnistetään valtion ympärivuorokautisen tietoturvatoiminnan jatkoselvittelyhanke. Väestörekisterikeskuksen kannalta on tärkeää, että palvelu on saatavissa ja että sen laatu on korkeatasoista. Pienellä virastolla ei yksinään ole mahdollista järjestää tällaista palvelua, vaan on järkevää, että palvelu on osa jonkin palvelukeskuksen toimintaa.

Väestörekisterikeskus pitää Poliisin tietohallintokeskusta mahdollisena ympärivuorokautisen tietoturvatoimintaa järjestävänä tahona.

LIITE 4 Voimassa oleva VAHTI-ohjeistus ja -julkaisut

VAHTI 4/2006: Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006: Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006: Electronic-mail Handling Instruction for State Government
VAHTI 1/2006: VAHTIn toimintakertomus vuodelta 2005
VAHTI 3/2005: Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005: Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005: Information Security and Management by Results
VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004: Datasäkerhet och resultatstyrning
VAHTI 3/2004: Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004: Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004: Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 6/2003: Opas julkishallinnon tietoturvakoulutuksen järjestämisestä
VAHTI 5/2003: Käyttäjän tietoturvaohje
Datasäkerhetsanvisning för användaren
User´s Information Security Instruction
VAHTI 4/2003: Valtionhallinnon tietoturvakäsitteistö
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointi
VAHTI 2/2003: Turvallisen etäkäytön arkkitehtuuri
VAHTI 1/2003: Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002: Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002: Etätyön tietoturvaohje
VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001: Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001: Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

VAHTI 3/2001: Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 2/2001: Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 3/2000: Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000: Valtion tietoaineistojen käsittelyn tietoturvaohje (uudistettavana)
VAHTI 2/1999: Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus (uudistettavana)

Ohjeisto löytyy VAHTIn Internet-sivuilta www.vm.fi/vahti ja ohjeita saa myös tilattua hyvin edullisesti painotalo Editasta.

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin: (09) 160 01
Telefaksi: (09) 160 33123
www.vm.fi

4/2006

SELVITYS VALTION YPÄRIVUORO-KAUTISEN TIETOTURVATOIMINNAN JÄRJESTÄMISESTÄ

ISBN 951-804-609-3 (nid.)
ISBN 951-804-610-7 (PDF)
ISSN 1455-2566