VALTIOVARAINMINISTERIÖ

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä

Statsrådets principbeslut om utvecklandet av informations-säkerheten inom stats-förvaltningen

7/2009 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä

7/2009 VAHTI

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila/VM-julkaisutiimi
ISSN 1455-2566 (nid)
ISBN 978-952-251-016-7 (nid)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-017-4 (pdf)

Painotuote

Edita Prima Oy
Helsinki 2009

Sisältö

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä

Valtioneuvosto on tänään valtioneuvoston ohjesäännön (262/2003) 3 §:n 11 kohdan nojalla päättänyt valtionhallinnon tietoturvallisuuden kehittämisperiaatteista.

1 Tavoite ja lähtökohdat

Tietoturvallisuuden hyvä hoitaminen on edellytys toimintojen ja palveluiden laadulle, tehokkuudella ja avoimuudelle, sidosryhmien luottamukselle hallinnon toimintaan sekä kansalaisten ja yhteisöjen eduille ja oikeuksille. Tietoturvatoiminnan tarkoituksena on tietojen sekä niiden käsittelyn, hallinnan ja käytön turvaaminen. Tietoturvallisuus liittyy kaikkiin prosesseihin, joiden avulla pyritään toteuttamaan kansanvallan kannalta tärkeitä yhteiskunnallisia arvoja. Oikeusvaltioperiaatteeseen kuuluu, että kaikessa toiminnassa on noudatettava lakia.

Periaatepäätöksellä ohjataan valtionhallintoa kehittämään tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä ja toimintaa. Riittävä resursointi tietoturvallisuuden kehittämiseen ja ylläpitoon on välttämätön edellytys toiminnalle sekä sen tehostamiselle ja tuottavuuden parantamiselle.

Periaatepäätöksellä ohjataan valtionhallinnon tietoturvallisuuden kokonaisuutta ja sen keskeisiä liittymäpintoja sidosryhmiin sekä vahvistetaan tie-

toturvayhteistyötä. Siinä päätetään kehittämisen periaatteista ja painopisteistä sekä linjataan keskeiset suuntaviivat jokaisen viranomaisen tietoturvatyölle.

Jokaisen viranomaisen tulee huolehtia siitä, että riittävän hyvä tietoturvallisuus ja henkilötietojen suoja toteutuvat omassa organisaatiossa ja yhteistyössä sidosryhmiensä kanssa sekä hankittaessa palveluita organisaation ulkopuolelta. Kansalaisille ja yhteisöille tarjottavien hallinnon palveluiden ja muun julkisen vallan käytön tulee tapahtua niin, että voidaan turvata riittävällä tavalla käytössä olevien tietojen, tuotettujen palveluiden ja järjestelmien tietoturvallisuus.

Riittävä tietoturvallisuuden, varautumisen ja suojauksen taso tulee määritellä ja toteuttaa ottaen huomioon asiaa koskevat säädökset ja käyttäen perustana kunkin organisaation toiminnallisia tavoitteita ja toimintojen tietosisällön arvoa ja merkitystä valtionhallinnolle, kansalaisille ja yhteisöille. Säädösten sekä organisaatiokohtaisten tavoitteiden, toimintojen ja tietojen lisäksi riittävän tietoturvallisuuden, varautumisen ja suojauksen tason määrittämisen ja toteuttamisen lähtökohtia ovat valtionvarainministeriön antamat tietoturvallisuuden ja varautumisen tasot ja -ohjeet.

2 Soveltamisala

Tämän valtioneuvoston periaatepäätöksen toteuttaminen on osa hyvän hallinnon periaatteita. Soveltamisala koskee kaikkia hallinnon palveluita, toimintoja, prosesseja, tietojärjestelmiä ja -verkkoja kattaen tiedon koko elinkaaren.

Periaatepäätös koskee valtion budjettitalouden piirissä olevia organisaatioita ja liikelaitoksia sekä näiden ulkopuolisilta tahoilta hankkimia tai perustamiinsa osakeyhtiöihin ulkoistamia toimintoja, prosesseja tai palveluja.

Periaatepäätöstä noudatetaan myös valtionhallinnon ja muiden organisaatioiden (kuten kunnat, yritykset ja yhteisöt) välisessä toiminnallisessa, tiedon hallinnan ja varautumisen yhteistyössä sekä kansainvälisessä yhteistyössä.

3 Kehittämisperiaatteet, -kohteet ja painopisteet

Valtionhallinnon tietoturvallisuutta vahvistetaan ja kehitetään osana toiminnan ja prosessien uudistamista ja hoitamista. Tietoturvallisuus on kes-

keinen ja kiinteä osa riskienhallintaa, hallinnon palveluita ja kehittämistä, resurssisuunnittelua sekä toiminnan sisäistä ja ulkoista tarkastusta.

Tietoturvallisuuden kehittäminen on jatkuvaa toimintaa, jonka **kehittämisperiaatteet** ovat:

- **Vastuullisuus:** Jokainen organisaatio vastaa tietoturvallisuutensa jatkuvasta ja ennakoivasta kehittämisestä. Johto ja henkilöstö vastaavat tehtäviensä tietoturvatoimenpiteistä ja raportoinnista. Organisaatioissa on oltava kuvattuna tietoturvallisuuden ja varautumisen vastuut.
- **Laillisuus:** Organisaatiot toimivat lainsäädännön ja Suomea koskevien kansainvälisten sopimusten tietoturvavelvoitteiden edellyttämällä tavalla. Tietoturvallisuutta ja varautumista koskeva lainsäädännön kokonaisuus selvitetään viranomaisyhteistyönä kehittämisen perustaksi.
- **Osaaminen:** Kaikilla esimiehillä ja työntekijöillä on tehtäviensä ja valtion tietoturvavaatimusten edellyttämä osaaminen. Tietoturvaosaamista arvioidaan tulos- ja kehityskeskusteluissa tehtäviin nähden. Jokaisen viranomaisen tulee aktiivisesti kehittää henkilökuntansa tietoturvatietoisuutta ja -koulutusta. Osaamista kehitetään ja seurataan valtionhallinnon tasolla.
- **Yhteistyö ja synergiaedut:** Hallinnon organisaatiot osallistuvat aktiivisesti valtionhallinnon tietoturvayhteistyöhön sekä toimivat tehtäviensä edellyttämässä yhteistyössä kuntien ja elinkeinoelämän kanssa. Eri henkilöryhmät kehittävät tietoturvallisuutta yhteistyössä ja organisaation eri toiminnot kattavasti Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn ohjeita sekä valtion tietoturvatasojen ja varautumisen määrityksiä hyödyntäen.
- **Integrointi:** Tietoturvallisuus koskee kaikkia toimintoja ja se on kiinteä osa viranomaisen koko toimintaa ja sen kehittämistä. Tietoturvallisuuden ja varautumisen toteutuminen varmistetaan toiminnoissa, prosesseissa, palveluissa ja hankinnoissa sekä hallinnon kehittämishankkeissa.
- **Kansainvälinen yhteistyö:** Kansainväliseen tietoturvayhteistyöhön osallistuvat organisaatiot vaikuttavat aktiivisesti eri toimintafoorumeissa tuoden osaltaan hyviä käytäntöjä valtionhallintoon.

Valtionhallinnon tietoturvallisuuden kehittämisen painopisteet ovat:

Johtaminen: Tietoturvallisuus integroituu osa-alueena johtamiseen, tulosohjaukseen ja resurssisuunnitteluun. Sen vastuiden tulee näkyä työjärjestyksissä ja toimenkuvissa. Johdon tehtävänä on vahvistaa osana toiminnan suunnittelua ja seurantaa organisaationsa tietoturvatavoitteet ja periaatteet sekä varmistaa organisaation toiminnan tietoturvallisuus ja sen edellyttämät resurssit. Jokainen esimies vastaa osaltaan siitä, että asetetut tietoturvavaatimukset toteutuvat.

Tietoturvallisuuden johtamisen kehittämiskohteita ovat

- tietoturvatoiminnan kattava sisällyttäminen tulosohjaukseen,
- selvitys tietoturvallisuuden johtamisesta, raportoinnista ja tarkastustoiminnasta,
- resurssien priorisointi tietoturvallisuuden ja varautumisen kannalta keskeisiin kohteisiin
- sekä tietoturvamittareiden kehittäminen ja käyttö johtamisessa.

Kokonaisvaltaisuus ja läpäisy: Organisaatiot kehittävät kokonaisvaltaisesti tietoturvallisuutensa hallintajärjestelmää, mittareita ja seurantaa sekä palvelu- ja hankintaketjujen tietoturvallisuuden ja varautumisen hallintaa. Viranomaisilla tulee olla valtiovarainministeriön VAHTI-ohjeisiin ja tietoturvatasomäärityksiin ja varautumistoiminnan vaatimuksiin perustuvat suunnitelmat, ohjeet ja menettelyt, joita auditoidaan keskitetysti.

Tietoturvatoiminnan kokonaisvaltaisuuden ja läpäisyn kehittämiskohteita ovat

- jokaisen organisaation tietoturvatoiminnan saaminen vähintään tietoturvatasomääritysten mukaiselle perustasolle,
- valtion kattavan VAHTI-ohjeiston kehittäminen, ylläpito ja jalkauttaminen toimintaan,
- valtionvarainministeriön tietoturvaohjeiden mukainen toiminta virastoissa,
- tietoturvallisuuden ja varautumisen valtiotason yhteishankkeiden toteuttaminen,
- tietoturvallisuuden ja varautumisen sisällyttäminen kehittämishankkeisiin sekä

- asiantuntijaresurssien ja osaamisen varmistaminen valtiotason tietoturva- ja varautumisyhteistyössä.

Ennaltaehkäisy ja varautuminen: Organisaatiot panostavat jatkuvaan ennakoivaan tietoturvatyöhön, toipumissuunnitteluun ja sen harjoitteluun sekä riskienhallintaan. Viranomaiset osallistuvat VAHTI-ohjeiden kehittämiseen ja hyödyntävät näitä ohjeita ennakoivassa tietoturvatyössä sekä parantavat häiriötilanteiden ja poikkeusolojen toimintavarmuutta.

Ennaltaehkäisevän tietoturvatoiminnan keskeisiä kehittämiskohteita ovat

- säädösvelvoitteiden mukainen tietoturvallisuuden toimeenpano,
- tietoturvallisuuden integroiminen kiinteäksi osaksi turvallisuustoiminnan kokonaisuutta,
- uhka- ja riskiarvioinnin metodiikan kehittäminen ja jatkuva riskienhallintatyö,
- toipumissuunnittelun tehostaminen yhteismitallisesti varautumistoiminnan kanssa sekä
- toipumis- ja jatkuvuussuunnitelmien harjoittelu.

Tiedon ja sen arvon suojaaminen: Organisaatiot parantavat tietoaineistojen, -järjestelmien ja -verkkojen turvallisuutta sekä kehittävät valtion ympärivuorokautista tietoturvatoimintakykyä. Organisaatiot toimivat valtion yhteisten varautumislinjausten, tietoaineistojen suojaustasojen ja tietoturvatasojen vaatimusten mukaisesti sekä ottavat käyttöön näitä tukevat tietotekniset ratkaisut.

Tiedon ja sen arvon suojaamisen kehittämiskohteita ovat

- tietojen omistajuuden ja vastuiden selkiyttäminen
- varautumisen linjausten ja tasojen sekä tietoaineistojen yhdenmukaisten suojaustasojen ja niiden edellyttäminen tietoturvakäytäntöjen kehittäminen ja käyttöönotto,
- valtionhallinnon turvallisten verkkoratkaisujen kehittäminen ja käyttöönotto sekä
- valtionhallintotason ympärivuorokautisen tietoturvatoiminnan toteuttaminen.

4 Tietoturvallisuuden yhteiskunnalliset toimijat

Valtiovarainministeriö

Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ohjaus- ja yhteensovittamisroolinsa toteuttamiseksi valtiovarainministeriö asettaa ja ylläpitää toimialallaan yhteistyön ohjaamiseen, kehittämiseen ja koordinaatioon tarvittavat toimielimet.

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI

Valtiovarainministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tietoturvallisuuden linjaukset.

Muut ministeriöt

Valtiovarainministeriön lisäksi erikseen määriteltyjä tietoturvallisuuden ohjaus- tai valvontatehtäviä on valtioneuvoston kanslialla, liikenne- ja viestintäministeriöllä, puolustusministeriöllä, oikeusministeriöllä, sisäasianministeriöllä ja ulkoasiainministeriöllä.

Viestintävirasto

Viestintävirasto toimii kansallisena tietoturvauhkia ja -loukkauksia käsittelevänä CERT-viranomaisena.

Palvelukeskukset

Valtiokonttoriin sijoitettu Valtion IT-palvelukeskus on palvelukeskusten piirissä keskeisessä roolissa tarjoten valtionhallinnon yksiköille tietotekniikan tietoturvallisuuteen liittyviä asiantuntija- ja muita palveluita. Hallinnonalojen sisäiset ja useita hallinnonaloja palvelevat palvelukeskukset ovat tiedonkäsittelyn suhteen keskeisessä asemassa valtionhallinnossa.

Muut tietoturvallisuuden yhteiskunnalliset toimijat

Arkistolaitoksella, Huoltovarmuuskeskuksella, Tietosuojavaltuutetun toimistolla ja Tietosuojalautakunnalla on työjärjestyksensä mukaisesti poik-

kihallinnollisesti tietoturvallisuuden kannalta keskeisiä nimettyjä tehtäviä. Muita poikkihallinnollisia tietoturvapalveluita tuottavia organisaatioita on sisäasiainministeriön ja puolustusministeriön hallinnonaloilla.

5 Päätöksen toimeenpano ja resurssit

Tietoturvallisuuden kehittäminen on jatkuvaa toimintaa. Kukin viranomainen vastaa omalta osaltaan päätöksen aktiivisesta toteuttamisesta, osallistuu yhteistyöhön ja hankkeisiin sekä seuraa tietoturvallisuuden kehitystä. Jokainen organisaatio sisällyttää tietoturvatoimenpiteiden tavoitteet ja resurssitarpeet tulosohjaukseen, toiminnan suunnitteluun, strategioihin ja talousarvioesityksiin.

Valtiovarainministeriö raportoi tämän päätöksen toimeenpanosta Hallinnon ja alueiden kehittämisen ministeriryhmälle ja antaa tarvittaessa periaatepäätökseen liittyviä ohjeita. Valtiovarainministeriö johtaa päätöksen toimeenpanoa, joka yhteensovitetaan ja koordinoidaan VAHTIssa.

Periaatepäätöksen toteuttamiseksi, tietoturvatyön tehostamiseksi, tietoturvauhkiin varautumisen vahvistamiseksi ja yhteistyön varmistamiseksi sekä kehittämisperiaatteiden, -kohteiden ja painopisteiden edistämiseksi viranomaiset toteutettavat ja resursoivat valtionhallinnon tietoturvallisuuden kehittämisohjelman vuosille 2010 - 2015. VAHTI valmistelee vuosittain toimintakertomuksen, johon sisältyy kehitysohjelman toteuttamisen ja vaikutuksen kuvaus.

Hallinnonalat kohdistavat varoja ja resursseja tietoturvallisuuden kehittämiseen ja VAHTIssa koordinoitavaan yhteistyöhön.

6 Tietoturvallisuuden raportointi ja valvonta

Viranomaiset raportoivat tietoturvatoiminnastaan valtiovarainministeriölle, Tietosuojavaltuutetulle sekä hallinnonalansa ministeriölle. Valtiontalouden tarkastusvirastolla on toimivalta tarkastaa hallinnon organisaatioiden toiminta kattaen tietoturvallisuuden. Käynnistettävässä tietoturvallisuuden kehittämisohjelmassa tullaan panostamaan myös tietoturvallisuuteen liittyvän raportointi- ja valvontamekanismin kehittämiseen.

7 Voimaantulo

Tämä päätös tulee voimaan 1. päivänä joulukuuta 2009 ja sillä kumotaan valtioneuvoston 11.11.1999 antama periaatepäätös valtionhallinnon tietoturvallisuudesta (VM 0024:00/02/99/1998).

Statsrådets principbeslut om utvecklandet av informationssäkerheten inom statsförvaltningen

Statsrådet har i dag i enlighet med 3 § 11 punkten i reglementet för statsrådet (262/2003) fattat beslut om utvecklingsprinciperna för statsförvaltningens informationssäkerhet.

1 Mål och utgångspunkter

En god skötsel av informationssäkerheten är en förutsättning för en god kvalitet på funktioner och tjänster, effektivitet och öppenhet, intressegruppernas förtroende för förvaltningens arbete samt för allmänhetens och sammanslutningars rättigheter och intressen. Informationssäkerheten har som mål att göra informationen samt behandlingen, hanteringen och användningen av informationen trygg. Informationssäkerheten anknyter till alla processer som syftar till att förverkliga viktiga demokratiska samhälleliga värden. I enlighet med rättsstatsprincipen ska lag iakttas i all verksamhet.

Genom principbeslutet styrs statsförvaltningen att utveckla informationssäkerheten som en viktig del av ledningen, riskhanteringen och utvecklandet av förvaltningen och dess verksamhet. Tillräckliga resurser för utvecklandet och upprätthållandet av informationssäkerheten är en viktig förutsättning för verksamheten och för förbättringen och effektiviseringen av verksamheten samt för en bättre produktivitet.

Principbeslutet styr både statsförvaltningens informationssäkerhet som helhet och de viktigaste kontakterna till intressegrupperna samt förstärker

informationssäkerhetssamarbetet. I beslutet fastställs principerna och tyngdpunkterna för utvecklingsarbetet och dras upp de centrala riktlinjerna för de enskilda myndigheternas informationssäkerhetsarbete.

Varje myndighet ska se till att en tillräckligt god nivå på informationssäkerheten och ett tillräckligt gott skydd av personuppgifter garanteras inom den egna organisationen och i samarbetet med intressegrupperna samt när tjänster skaffas utanför organisationen. När myndigheterna erbjuder allmänheten och sammanslutningarna förvaltningstjänster och utövar annan offentlig makt ska det ske på ett sådant sätt att informationssäkerheten för informationen, de tjänster som tillhandahålls och de system som används säkerställs i tillräckligt hög grad.

En tillräckligt hög nivå på informationssäkerheten, beredskapen och skyddet ska fastställas och genomföras så att författningar följs och så att dessa åtgärder grundar sig på organisationernas operativa mål och värderingarna i faktainnehållet i funktionerna och dess betydelse för statsförvaltningen, allmänheten och samfunden. Utöver författningar och organisationernas egna mål, funktioner och information är de nivåer och anvisningar som finansministeriet gett i fråga om informationssäkerheten och beredskapen utgångspunkter när man ska fastställa och genomföra en tillräcklig nivå på informationssäkerheten, beredskapen och skyddet.

2 Tillämpningsområde

Detta statsrådets principbeslut genomförs som en del av principerna för god förvaltning. Beslutet tillämpas på förvaltningens alla tjänster, funktioner, processer, informationssystem och informationsnät, och på ett sådant sätt att det täcker hela livscykeln för informationen.

Principbeslutet tillämpas vid alla de organisationer och affärsverk som omfattas av statens budgetekonomi samt i funktioner, processer eller tjänster som dessa har upphandlat av utomstående parter eller som lagts ut på entreprenad i aktiebolag som grundats.

Principbeslutet ska också efterföljas i sådant samarbete mellan statsförvaltningen och andra organisationer (t.ex. kommuner, företag och samfund) som gäller det operativa samarbetet eller samarbete som gäller informationshantering och beredskap samt i internationellt samarbete.

3 Utvecklingsprinciper, utvecklingsmål och tyngdpunkter

Som en del av skötseln och förnyandet av verksamheten och processerna inom statsförvaltningen kommer man att stärka och utveckla informationssäkerheten. Informationssäkerheten är en viktig och fast del av riskhanteringen, förvaltningens tjänster och utveckling, resursplaneringen samt den interna och externa revisionen av verksamheten.

Utvecklandet av informationssäkerheten är en fortgående verksamhet, som har följande **utvecklingsprinciper:**

- **Ansvarighet:** Varje organisation ska ansvara för att den egna informationssäkerheten utvecklas kontinuerligt och på ett förutseende sätt. Ledningen och personalen ansvarar för informationssäkerhetsåtgärder i sina egna arbetsuppgifter och rapporterar om dem. I organisationen ska finnas en beskrivning över ansvarsfördelningen när det gäller informationssäkerheten och beredskapen.
- **Laglighet:** Organisationernas arbete ska vara förenligt med lagstiftningen och följa de internationella avtal om informationssäkerhet som Finland har ingått. Som en grund för utvecklandet kommer myndigheterna gemensamt att se över hela lagstiftningen gällande informationssäkerheten och beredskapen.
- **Kompetens:** Alla chefer och anställda ska ha de kunskaper som deras arbetsuppgifter och statens informationssäkerhetskrav förutsätter. I samband med resultat- och utvecklingssamtalen bedöms informationssäkerhetskompetensen med tanke på arbetsuppgifterna. Alla myndigheter ska aktivt utveckla personalens medvetenhet om informationssäkerhet och utbildning i informationssäkerhetsfrågor. Kompetensen utvecklas och följs upp på statsförvaltningsnivå.
- **Samarbete och synergieffekter:** Organisationerna inom förvaltningen ska aktivt delta i statsförvaltningens informationssäkerhetsarbete och samarbetar med kommunerna och näringslivet i sådant samarbete som deras uppgifter förutsätter. Informationssäkerheten utvecklas i samarbete mellan olika persongrupper så att den täcker alla funktioner i organisationen. I detta arbete utnyttjas ledningsgruppen för datasäkerheten

inom statsförvaltningen VAHTI:s anvisningar och statens informationssäkerhetsnivåer samt definitioner på beredskapen.

- **Integrering:** Informationssäkerheten gäller alla funktioner och den är en fast del av myndighetens hela verksamhet och av dess utvecklande. Att informationssäkerhet och beredskap uppnås säkerställs i funktionerna, processerna, tjänsterna och anskaffningarna samt i förvaltningens utvecklingsprojekt.
- **Internationellt samarbete:** Organisationer som deltar i internationellt informationssäkerhetssamarbete deltar aktivt i olika verksamhetsforum och tar in god praxis inom statsförvaltningen.

Statsförvaltningen har följande prioritetsområden när det gäller utvecklandet av informationssäkerheten:

Styrningen: Informationssäkerheten ska integreras som ett delområde av styrningen, resultatstyrningen och resursplaneringen. Ansvaret bör framgå av arbetsordningarna och befattningsbeskrivningarna. Det är ledningens uppgift att som en del av verksamhetsplaneringen och uppföljningen stärka målen och principerna för informationssäkerheten inom den egna organisationen, samt att säkerställa informationssäkerheten inom organisationens verksamhet och de resurser som detta kräver. Alla chefer ansvarar för att de informationssäkerhetskrav som ställts genomförs.

Följande utvecklingsområden ställs upp för styrningen av informationssäkerheten

- att informationssäkerheten ingår i resultatstyrningen på ett täckande sätt
- en utredning om styrningen och rapporteringen av informationssäkerheten och av revisionsverksamheten
- att resurserna riktas till prioriterade centrala områden med tanke på informationssäkerheten och beredskapen
- att mätare för informationssäkerheten utvecklas och används i styrningen.

Helhet och verkan: Organisationerna ska utveckla sina informationssäkerhetssystem och informationssäkerhetsmätare och uppföljningen av dem samt hanteringen av informationssäkerheten när det gäller tjänste- och anskaffningskedjor och beredskap på ett övergripande sätt. Myndigheterna bör ha planer, anvisningar och förfaranden som grundar sig på finansmins-

teriets VAHTI-anvisningar och på krav om bestämmelser om informationssäkerhetsnivån och beredskapsverksamheten, som kvalitetsrevideras centraliserat.

Följande utvecklingsområden ställs upp för att informationssäkerheten ska vara helhetsbetonad och verkningsfull

- att samtliga organisationers informationssäkerhet ska nå minst den grundnivå som ställts upp för informationssäkerhetsbestämmelser
- att riksomfattande VAHTI-anvisningar utvecklas, uppdateras och förankras i verksamheten
- att ämbetsverken iakttar finansministeriets informationssäkerhetsanvisningar i sin verksamhet
- att gemensamma projekt om informationssäkerheten och beredskapen genomförs på riksnivå
- att utvecklingsprojekten inbegriper informationssäkerhet och beredskap samt
- att expertresurser och kompetens säkerställs genom samarbete inom informationssäkerhetsarbetet och beredskapsarbetet.

Förebyggande och beredskap: Organisationerna satsar på ett kontinuerligt informationssäkerhetsarbete, återhämtningsplanering och övningar samt riskhantering. Myndigheterna deltar i utvecklandet av VAHTI-anvisningar och använder dessa anvisningar i förebyggande informationssäkerhetsarbete, och förbättrar funktionssäkerheten vid störningssituationer och undantagsförhållanden.

Följande centrala utvecklingsområden ställs upp för en förebyggande informationssäkerhetsverksamhet

- att informationssäkerheten genomförs enligt förpliktelser enligt lag
- att informationssäkerheten integreras som en fast del av hela säkerhetsverksamheten
- att utveckla hot- och riskbedömningens metodik och ett kontinuerligt rikshanteringsarbete
- att återhämtningsplaneringen effektiveras i samma omfattning som beredskapsverksamheten

- att återhämtnings- och kontinuitetsplanerna övas.

Skyddet av information och av informationsvärdet: Organisationerna ska förbättra säkerheten för sitt informationsmaterial, sina datasystem och datanät samt utvecklar en beredskap att upprätthålla informationssäkerhetsverksamet dygnet runt. Organisationernas verksamhet är förenlig med statens gemensamma principer för beredskap och nivån på skyddet av information. Organisationerna tillämpar också datatekniska lösningar som stöder dessa.

Följande utvecklingsområden ställs upp för skyddet av information och av informationsvärdet

- att ägandet av och ansvaret för information tydliggörs
- att utveckla och ta i bruk principer och nivåer i fråga om beredskapen samt harmoniserade skyddsnivåer för informationsmaterialet och av informationssäkerhetspraxis som krävs för dessa
- att utveckla och ta i bruk säkra nätlösningar för statsförvaltningen och
- att se till att informationssäkerhetsverksamheten på statsförvaltningsnivå fungerar dygnet runt.

4 Samhälleliga informationssäkerhetsparter

Finansministeriet

Finansministeriet leder och samordnar utvecklandet av den offentliga förvaltningens och särskilt statsförvaltningens informationssäkerhet. I denna roll som ledare och samordnare tillsätter och upprätthåller finansministeriet inom sitt verksamhetsområde sådana organ som behövs för ledningen, utvecklingen och samordningen av detta samarbete.

Ledningsgruppen för datasäkerheten inom statsförvaltningen VAHTI

Den av finansministeriet tillsatta ledningsgruppen för datasäkerheten inom statsförvaltningen VAHTI är ett organ för samarbetet, styrningen och utvecklandet av datasäkerheten inom förvaltningen. VAHTI behandlar alla viktiga riktlinjer för informationssäkerheten inom statsförvaltningen.

Övriga ministerier

Utöver finansministeriet har statsrådets kansli, kommunikationsministeriet, försvarsministeriet, justitieministeriet, inrikesministeriet och utrikesministeriet särskilt fastställda styrnings- och övervakningsuppgifter inom informationssäkerheten.

Kommunikationsverket

Kommunikationsverket är den nationella CERT-myndigheten som behandlar hot och kränkningar mot informationssäkerheten.

Servicentraler

Statens IT-servicecentral, som är placerad vid Statskontoret, är en central servicecentral då den erbjuder experttjänster och övriga tjänster som anknyter till informationsteknisk säkerhet för enheterna inom statsförvaltningen. De servicecentraler som finns inom förvaltningsområdena och som betjänar flera förvaltningsområden är i central ställning i statsförvaltningen när det gäller informationsbehandling.

Andra samhälleliga informationssäkerhetsparter

Arkivverket, Försörjningsberedskapscentralen, Dataombudsmannens byrå och Datasekretessnämnden har i enlighet med sina arbetsordningar tväradministrativa, särskilt angivna uppgifter som är centrala med tanke på informationssäkerheten. Andra organisationer som tillhandahåller tväradministrativa informationssäkerhetstjänster finns inom inrikesministeriets och försvarsministeriets förvaltningsområden.

5 Beslutets genomförande och resurser

Informationssäkerheten är en verksamhet som utvecklas kontinuerligt. Varje myndighet svarar för sin del för att beslutet genomförs aktivt, deltar i samarbete och i olika projekt samt följer hur informationssäkerheten utvecklas. Varje organisation innefattar målen och behoven av resurser för informationssäkerhetsåtgärderna i sin resultatstyrning, verksamhetsplanering, sina strategier och budgetförslag.

Finansministeriet rapporterar om genomförandet av detta beslut till Ministerarbetsgruppen för förvaltning och regional utveckling och ger vid behov anvisningar i anslutning till principbeslutet. Finansministeriet leder beslutets genomförandet, som samordnas i VAHTI.

För att genomföra principbeslutet, effektivisera informationssäkerhetsarbetet, stärka beredskapen inför informationssäkerhetshot och för att säkerställa samarbete, samt för att främja utvecklingsprinciperna och målen för utvecklingen och tyngdpunkterna genomför och allokerar myndigheterna resurser för utvecklingsprogrammet för informationssäkerheten inom statsförvaltningen 2010 – 2015.

Förvaltningsområdena ger medel och resurser till utvecklandet av informationssäkerheten och till samarbete som samordnas inom VAHTI.

6 Rapportering och övervakning gällande informationssäkerheten

Myndigheterna rapporterar om informationssäkerhetsverksamheten till finansministeriet, Dataombudsmannen och ministerierna inom sina förvaltningsområden. Statens revisionsverk har befogenheter att granska verksamheten inom förvaltningens organisationer, inklusive informationssäkerheten. I det utvecklingsprogram för informationssäkerheten som inleds, kommer man också att fokusera på utvecklandet av rapporterings- och övervakningsmekanismen i fråga om informationssäkerheten.

7 Ikraftträdande

Detta beslut träder i kraft den 1 december 2009, och genom det upphävs statsrådets principbeslut om informationssäkerheten inom statsförvaltningen av den 11 november 1999 (FM 0024:00/00/02/99/1998).

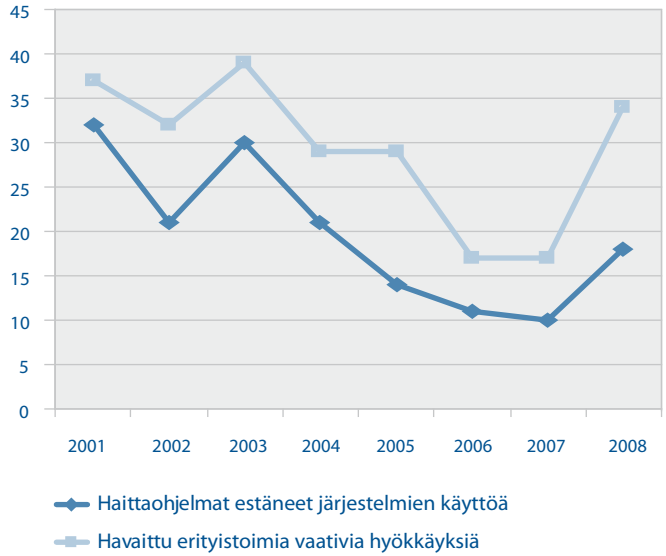
Liite 1

Valtioneuvoston periaatepäätöksen esittelymuistio

Valtiovarainministeriön (VM) ja Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) seuranta osoittavat tarvetta voimakkaasti kehittää valtion tietoturvallisuutta sekä ICT-varautumista koko valtionhallinnon, hallinnonalojen ja yksittäisten virastojen tasolla.

Tietoturvaongelmien kielteiset vaikutukset valtionhallinnon toimintaan, palveluihin ja järjestelmiin ovat yleistyneet ja pahenemassa. Alla olevasta kuvasta näkyy haittaohjelmista aiheutuneen järjestelmien käytön estymisen ja erityistoimia vaatineiden tietoturvahyökkäysten yleisyyden kehitys vuosina 2001 – 2008. Kuva kertoo vuosittaisen prosenttiosuuden VM:n tai VAHTIn kyselyyn vastanneista valtion organisaatioista, joilla on ollut näitä ongelmia. Tilannetta saatiin väliaikaisesti ja laajalla rintamalla paremmaksi VM:n johtaman vuosien 2004 – 2006 valtion tietoturvallisuuden kehitysohjelman aikana. Kehitysohjelma sisälsi kaikkiaan 28 kehittämiskohdetta, joista osa toimeenpantiin erityisten työryhmien tai jaostojen avulla ja osa yhteistyössä muilla toimenpiteillä.

Kuva 1. Haittaohjelmien ja tietoturvahyökkäysten vaikutusten yleisyys valtionhallinnossa.



Tietoturvallisuuden hyvä taso on tärkeä niin kansalaisten kuin hallinnon ja sen julkisuuskuvan kannalta. Puutteellinen tietoturvallisuus vaarantaa sekä kansalaisten että julkishallinnon turvallisuutta ja taloudellisia etuja. Lisäksi vahinkojen ja tiedonmenetysten kautta puutteellinen tietoturvallisuus aiheuttaa lisätyötä ja -kustannuksia sekä heikentää viranomaisen uskottavuutta ja kansalaisten luottamusta sähköisiin palveluihin.

Luottamus hallinnon toimintaan ja palveluihin edellyttää hyvää tietoturvallisuutta keskeisenä osana toiminnan ja palveluiden laatua. Sähköisen asioinnin turvallisuuden kehittäminen ja ylläpitäminen vaativat nykyistä enemmän riskienhallinnan ja tietoturvallisuuden asiantuntemusta. Näin voidaan taata kansalaisten luottamus sähköiseen asiointiin ja saada käyttöön palveluita osana valtionhallinnon tuottavuusohjelmaa.

Käytetyillä valtiotason tietoturvallisuuden ohjauksen toimintamalleilla, kuten laajalla informaatio-ohjauksella ja yhteisillä hankkeilla sekä hajautuneella lainsäädännöllä ja työnjaolla, aikaansaatu parantaminen on liian hidasta verrattuna tietoturvallisuuden keskeiseen merkitykseen hallinnon toiminnalle ja tietoturvaongelmien haittavaikutuksiin. Merkittävä osa toi-

mijoista ei ole saanut aikaan riittävää tietoturvallisuutta toiminnoissaan eikä järjestelmissään. Tietoturvauhkien pahentuessa ja niiden ollessa entistä haasteellisimpia, on suunnitelmallisesti parannettava tietoturva- ja varautumistyötä ja johtamista.

Edellinen periaatepäätös valtionhallinnon tietoturvallisuudesta hyväksyttiin vuonna 1999. Täysin uudistettu periaatepäätös on valmistelu laajassa viranomaisyhteistyössä ja VM:n johdolla VAHTIssa. Periaatepäätöksen sisältöön ovat vaikuttaneet kaikki keskeiset viranomaiset. Periaatepäätös viimeisteltiin hallinnon ja aluekehityksen ministeriryhmän, valtiovarainministeriön johdon sekä avoimen ja laajan lausuntokierroksen palautteiden pohjalta.

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä on tärkeä osa hallituksen politiikkaa hallinnon ja tietoyhteiskunnan kehittämiseksi. Valtioneuvosto teki aiemmin periaatepäätöksen kansallisesta tietoturvastrategiasta vuonna 2008. Valtionhallinnon tietoturvallisuutta koskeva periaatepäätös on linjassa kansallisen strategian ja valtioneuvoston muiden linjausten kanssa sekä vahvistaa kansallisen tietoturvastrategian mukaista toimintaa valtionhallinnossa.

1 Periaatepäätöksen tavoite ja lähtökohdat

Valtionhallinnon tietoturvallisuutta koskevalla periaatepäätöksellä ohjataan valtionhallintoa kehittämään tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä ja toimintaa. Periaatepäätös edistää osaltaan valtion ja erilaisten yhteisöjen tietoturvallisuuden sekä kansalaisten perusoikeuksien ja tietosuojan toteutumista viranomaisten tietojärjestelmissä ja julkisissa palveluissa.

Tietoturvallisuuden hyvä hoitaminen on edellytys toimintojen ja palveluiden laadulle, tehokkuudella ja avoimuudelle, sidosryhmien luottamukselle hallinnon toimintaan sekä kansalaisten ja yhteisöjen eduille ja oikeuksille. Periaatepäätöksellä ohjataan valtionhallinnon tietoturvallisuuden kokonaisuutta ja sen keskeisiä liittymäpintoja sidosryhmiin sekä vahvistetaan tietoturvayhteistyötä.

Tietoturvatoiminnan tavoitteena on huolehtia palveluiden ja järjestelmien laadusta sekä varmistaa kansalaisten ja yhteisöjen edut ja oikeudet. Tietoturvallisuus liittyy kulloinkin kyseessä oleviin prosesseihin, joiden avulla pyritään toteuttamaan kansanvallan kannalta tärkeitä yhteiskunnallisia arvoja.

Näitä arvoja ovat esimerkiksi kansalaisten osallistumismahdollisuuksien turvaaminen, luottamus, turvallisuus, uskottavuus, avoimuus sekä henkilötietojen ja salassa pidettävien tietojen suoja.

Oikeusvaltioperiaatteeseen kuuluu, että kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Kansalaisille ja yhteisöille tarjottavien hallinnon palveluiden ja muun julkisen vallan käytön tulee tapahtua niin, että samalla voidaan turvata riittävällä tavalla käytössä olevien tietojen, niillä tuotettujen palveluiden ja niiden käsittelyyn osallistuvien järjestelmien tietoturvallisuus.

2 Soveltamisala

Päätöksen soveltamisala koskee kaikkia hallinnon palveluja, toimintoja, -prosesseja, tietojärjestelmiä ja -verkkoja kattaen tiedon koko elinkaaren. Soveltamisalaan kuuluu myös varautuminen tietohallinnon ja tietotekniikan riskeihin sekä niistä aiheutuvien häiriötilanteiden hallintaan. Periaatepäätös painottaa valtionhallinnon sisäisen tietoturvatyön lisäksi yhteistyötä sidosryhmien kanssa kattaen esimerkiksi toiminnallisen, tiedon hallinnan, varautumisen ja kansainvälisen yhteistyön sekä ulkoistetut toiminnot, prosessit ja palvelut.

Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta.

Tietoturvallisuuden keskeisillä käsitteillä tarkoitetaan seuraavaa:

Luottamuksellisuus; tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen käytettävissä. Sivullisille ei anneta mahdollisuutta muuttaa tai tuhota tietoja, eikä muutoin käsitellä tietoja.

Eheys; tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena.

Käytettävyys; järjestelmien tiedot ja palvelut ovat niihin oikeutettujen käytettävissä etukäteen määritellyssä vasteajassa. Tiedot eivät ole tuhoutuneet tai tuhottavissa vikojen, tapahtumien tai muun toiminnan seurauksena.

Todentaminen (autentikointi) tarkoittaa osapuolten (henkilö tai järjestelmä) luotettavaa tunnistamista esimerkiksi sähköisessä asiointipalvelussa ja tietojen siirrossa.

Kiistämättömyys tarkoittaa tapahtuneen todistamista jälkeenpäin, jolloin tavoitteena on juridinen sitovuus. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa jälkeenpäin.

3 Kehittämisperiaatteet, -kohteet ja painopisteet

3.1 Kehittämisperiaatteet

Tietoturvallisuus on keskeinen ja kiinteä osa riskienhallintaa, hallinnon palveluita ja kehittämistä, resurssisuunnittelua sekä toiminnan sisäistä ja ulkoista tarkastusta. Hallinnon toiminnan laatu, jatkuvuus, tehokkuus ja riskienhallinta edellyttävät, että valtionhallinnon toimijat kehittävät tietoturvallisuutta ja siihen liittyvä yhteistyötä jatkuvana toimintana ja hyviin käytäntöihin perustuen. Hyvät käytännöt kuvataan periaatepäätöksessä tiiviisti kehittämisperiaatteina, joiden mukaisilla menettelytavoilla tietoturvallisuutta vahvistetaan ja kehitetään osana toiminnan ja prosessien uudistamista ja hoitamista.

Kehittämisperiaatteet on muodostettu siten, että tavoitellaan tietoturvatyön tuloksellisuutta ja vaikuttavuutta. Kehittämisperiaatteissa on otettu huomioon kansalliset ja kansainväliset linjaukset ja hyvät käytännöt.

Vastuullisuusperiaate korostaa jokaisen toimijan vastuuta oman toimintansa ja järjestelmiensä tietoturvallisuudesta. Vastuuta ei voi ulkoistaa edes silloin, kun osia toiminnoista hoidetaan palveluverkoston avulla.

Laillisuusperiaatteen mukaan hallinto ja sen yhteistyökumppanit toimivat kansallisen lainsäädännön ja Suomea koskevien kansainvälisten tietoturvavelvoitteiden edellyttämällä tavalla. Useat lait, asetukset ja määräykset sisältävät viranomaisia koskevia tietoturvavelvoitteita ja velvoittavat huolehtimaan tietojen luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä tietojen saatavuudesta hallinnonalojen eri rekistereistä. Esimerkkejä keskeisistä valtionhallinnon tietoturvatoimintaa ohjaavista säädöksistä ovat:

- perustuslaki (731/1999)
- arkistolaki (831/1994)
- henkilötietolaki (523/1999)

- laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- laki valtion talousarviosta (423/1988)
- asetus valtion talousarviosta (1243/1992)
- laki viranomaisen toiminnan julkisuudesta (621/1999)
- asetus viranomaisten toiminnan julkisuudesta (1030/1999)
- laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
- laki turvallisuusselvityksistä (177/2002)
- viestintämarkkinalaki (393/2003)
- laki yksityisyyden suojasta työelämässä (759/2004)
- sähköisen viestinnän tietosuojalaki (516/2004)
- valmiuslaki (1080/1991)
- valtion virkamieslaki (750/1994)
- laki valtion liikelaitoksista (1185/2002).

Laaja ja useisiin säädöksiin hajautunut kokonaisuus tulee selvittää viranomaisyhteistyönä tietoturvakehittämisen vahvistamiseksi ja johtamisen kehittämiseksi. Hajautunut lainsäädäntö saattaa olla riski vakavien häiriötilanteiden ja kriisien hallinnalle sekä johtamiselle.

Osaamisperiaate painottaa tarvetta vahvistaa tietoturva- ja varautumisosaamista koko valtionhallinnon ja sen koko henkilökunnan laajuisesti. Tehtävän edellyttämä tietoturvaosaaminen tulee hallinnossa olla johdon ja työntekijöiden perustaito. Edessä olevat eläköitymiset ja henkilöiden vaihdokset tekevät valtionhallintotasoisen osaamisen kehittämisen välttämättömäksi. Hallinnon ICT-henkilökunnan työajankäyttöä ja osaamista tulee laajassa mitassa siirtää perustietotekniikkatehtävistä tietoturvallisuuteen, varautumiseen sekä tietotekniikan ja tietohallinnon ohjaamiseen.

Yhteistyön ja synergiaetujen periaate tarkoittaa aktiivista yhteistyötä valtionhallinnossa ja myös kuntien ja elinkeinoelämän kanssa. Yhteistyön tuloksena hyvien käytäntöjen mukainen toiminta laajenee, tuottavuus paranee ja yhteisten linjausten toimeenpano vauhdittuu. Esimerkiksi VAHTI-yhteistyöllä on saatu aikaan merkittävää tietoturvallisuuden paranemista. Synergiaetujen vuoksi tulee varmistaa parhaan mahdollisen asiantuntijahenkilöstön tasainen saatavuus ja käyttö yhteisissä hankkeissa.

Integrointiperiaate tarkoittaa tietoturvallisuuden ja varautumisen toteutumista toiminnoissa, prosesseissa, palveluissa ja hankinnoissa sekä hallinnon ja ICT:n kehittämishankkeissa. Tietoturvallisuus ja varautumisasioiden läpikäynti tulee aloittaa kehittämistyön alussa.

Suomen tulee toimia aktiivisesti *kansainvälisessä tietoturvayhteistyössä*. Valtiot, yritykset ja kansainväliset järjestöt edellyttävät Suomelta ja muilta yhteistyökumppaneiltaan turvallisuuden hyvää hoitamista. Kansainvälisessä tietoturvayhteistyössä toimii nykyisin lähes 20 valtionhallinnon organisaatiota. Tavoite on, että kansainväliseen tietoturvayhteistyöhön osallistuvat organisaatiot vaikuttavat aktiivisesti eri toimintafoorumeissa tuoden osaltaan hyviä käytäntöjä valtionhallintoon. Yhteistyön koordinaatiota tulee tehostaa.

3.2 Painopisteet

Kehittämisen painopisteiden valinnan kriteerejä ovat kehittämisen vaikuttavuus sekä perusteellisesti ja ongelmienkin kautta analysoitu tarve valtiotasoille kehittämiselle ja yhteistyölle. Valittuna on rajallinen määrä painopisteitä ja kehittämisen kohteita, joihin panostetaan. Painopisteet ovat johtaminen, kokonaisvaltaisuus ja läpäisy, ennaltaehkäisy ja varautumien sekä tiedon ja sen arvon suojaaminen.

Valtionhallinnossa on kesken tietoturvatyön resursointi ja sisällyttäminen tulosohjaukseen sekä toiminnan suunnitteluun. Näihin liittyvät toimenpiteet on eri organisaatioissa huomioitu vaihtelevasti. Vuonna 2008 tietoturvatavoitteet oli viety tulosohjaukseen noin 38 prosentilla VAHTIn kyselyyn vastanneista valtion organisaatioista. Puutteita on myös prosessien ja niiden riippuvuuksien tunnistamisessa ja riskienhallinnassa, tietoturvallisuuden organisoinnissa, resurssoinnissa ja arvioinnissa, toipumis- ja jatkuvuussuunnittelussa sekä hankintaketjujen, tietojärjestelmien ja verkkojen turvallisuuden hallinnassa.

Johtaminen

Tietoturvallisuus on organisaation toiminnan yksi perusvaatimus ja laatutekijä, joka ei toteudu itsestään. Tietoturvallisuuden ja varautumisen nivominen johtamiseen on edellytys muiden painopisteiden tehokkaalle kehittämiselle. Jokainen johtaja ja esimies vastaa omalta osaltaan siitä, että tietoturvavaatimukset toteutuvat henkilöstön toiminnassa ja ne ovat kuvattuna työjärjestyksissä ja tehtäväkuvissa. Turvallisuuteen sitoutuminen ilmenee mm. organisaation turvallisuustoiminnan, tietohallinnon, arkistotoimen,

asiakirjahallinnon, tietopalvelun ja viestinnän riittävänä resursointina sekä selkeänä organisointina.

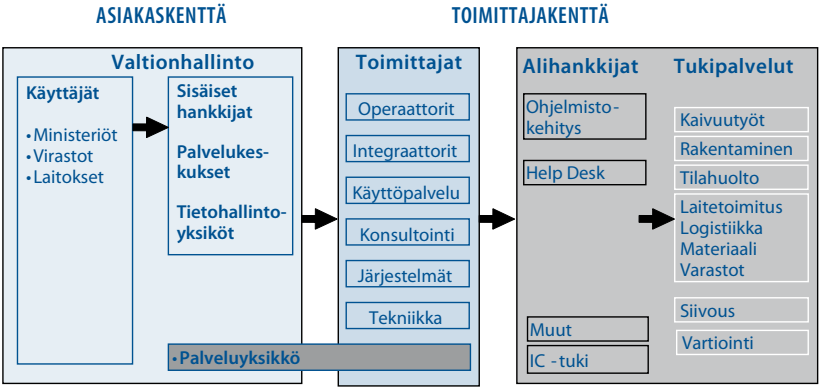
Toimintojen varmistaminen, riskienhallinta, laatu ja varautuminen edellyttävät resurssien priorisointia tietoturvallisuuden kannalta keskeisiin kohteisiin. Esimerkiksi kokopäivätoimisia tietoturvavastaavia on edelleen liian vähän koko valtionhallinnon tasolla. Vastuu tilanteen parantamisesta on jokaisen ministeriön ja viraston johdolla.

Johtamistoiminnan kehittämiseksi sekä mahdollisten katvealueiden kartoittamiseksi ja hallitsemiseksi valtionhallinnossa on tehtävä selvitys tietoturvallisuuden johtamisesta, raportoinnista ja tarkastustoiminnasta.

Kokonaisvaltaisuus ja läpäisy

Jokaisella organisaatiolla on velvoite kehittää tietoturvallisuutta. Kehittämisen perustana valtionhallinnossa ovat säädökset, VAHTIn ohjeet (www.vm.fi/vahti) sekä VM:n asettamat tietoturvatasojen ja varautumisen vaatimukset. Säädösten ja ohjeistuksen toimeenpanossa on merkittäviä eroja hallinnonalojen ja virastojen kesken.

Kuva 2. Esimerkkikuva palveluketjun hallinnasta



Oheisessa kuvassa on esimerkki palveluketjusta ja siihen sisältyvistä toimijoista. Katvealueeksi voi muodostua etenkin erilaisten palveluketjujen hallinta sekä niiden tilannekuva, jonka avulla hallinnon toimivuus voidaan varmistaa häiriötilanteissakin. Tietoturvallisuuden ja varautumisen hallintaa palveluketjuissa tulee kehittää.

Hallinnossa tulee varmistaa tietoturvallisuuden perustason toteutuminen koko valtionhallinnossa ja korotetun / korkean tason toteutuminen yhteiskunnan elintärkeissä toiminnoissa. Jokaisen hallinnon organisaation on saavutettava vähintään tietoturvallisuuden perustaso. VM antaa lähiaikoina ohjeen tietoturvatasoista ja niiden vaatimuksista. Tietoturvatasojen ja varautumisen toimeenpanoa tehostetaan yhteishankkeiden avulla.

Ennaltaehkäisy ja varautuminen

Valtionhallinnon organisaatiot tuottavat ennaltaehkäisyä tukevia välineitä turvallisuuden ja tietoturvallisuuden edistämiseksi. Näitä ovat VAHTI-ohjeet, tietojärjestelmäluokitukset, koulutusmateriaalit, erilaiset kampanjat sekä osallistuminen muiden viranomaisten kampanjoihin ja teematilaisuuksiin.

Toimintojen riskien hallitsemiseksi ja jatkuvuuden varmistamiseksi Suomen valtionhallinnon on jatkossa merkittävästi pystyttävä parantamaan tietoturvaongelmiin varautumista ja poikkeamatilanteiden hallintaa sekä tietojärjestelmien ja - verkkojen tilanteiden tuntemista ja hallintaa.

Hallinnossa käytettäviä riskienhallintamenettelyjä on kehitettävä ja yhteensovitettava kattaen kriittisen tietotekniikan tunnistamisen, varautumisen vaatimukset ja häiriötilanteista toipumisen. Nykyisin näiden puuttuessa vaatimuksien ja organisaation toiminnan tarpeiden välille saattaa muodostua katve Yhteiskunnan elintärkeiden toimintojen strategian (YETTS) mukaisissa turvallisuustilanteissa. Organisaatioiden toipumissuunnittelua ja varautumisharjoittelua on tehostettava.

Ennaltaehkäisyä palvelee riittävästi resursoitu NSA- ja DSA-toiminta (mukaan lukien tietoliikenneturvallisuusviranomainen NCSA) sekä valtionhallinnon keskitetyt turvallisuussopimukset YETTS:n kannalta keskeisten palveluiden tuottajien kanssa. NSAlla tarkoitetaan kansallista turvallisuusviranomaista (National Security Authority). DSA on määrätty turvallisuusviranomainen (Designated Security Authority).

Lakiin viranomaistoiminnan julkisuudesta perustuvalla annettavalla tietoturvallisuusasetuksella sekä siihen pohjautuvalla ohjeistuksella yhdenmukaistetaan luokiteltavan tietoaineiston käsittelyä ja suojaamismenettelyitä. Tämä on mittava ja hyvin tärkeä ponnistus, johon tulee panostaa lähivuosina.

Valtionhallinnon tietoverkkojen turvaamiseksi on VM:n ohjauksessa meneillään laaja ja keskeinen hanketyö. Hankkeen tuloksilla parannetaan tietojen ja valtion tuotannontekijöiden suojaa ja siten koko valtionhallinnon toimivuutta. Hankkeen tulokset varmistavat tietojen saatavuuden ja käytettävyyden myös häiriötilanteissa.

Vain osalla valtion organisaatioista on olemassa 24/7 -toimintakyky. Katvealueen poistamiseksi Suomen valtionhallinnon tulee lähivuosina saada aikaiseksi ja riittävän vahvasti resurssoiduksi ympärivuorokautinen tietoturvallisuuden valvonta- ja reagointikyky tarkemmin määriteltävässä laajuudessa. VAHTIssa tehty pohjatyö on dokumentoitu VAHTIn julkaisuihin 4/2006 ja 5/2008.

4 Tietoturvallisuuden yhteiskunnalliset toimijat

Hallitusohjelman kohdassa 7.2 hallitus sitoutuu edistämään kansalaisten ja yritysten luottamusta arjen tietoyhteiskunnan palveluihin keinoin, joita ovat yritysten toiminta-edellytyksien varmistaminen kaikissa oloissa kriittisen infrastruktuurin toimintavarmuutta ja yrityssalaisuuksien suojaa kehittämällä.

Nykyisen työnjaon mukaan tietoturvallisuus ja tietoturvallisuuden kehittäminen kuuluvat voimassa olevan lainsäädännön mukaan usean toimijan vastuulle. Valtioneuvoston ohjesääntöön (262/2003) on kirjattu ministeriöiden työnjako.

Tietoturvallisuuden yhteiskunnalliset toimijat luetteloidaan periaatepäätöksessä nykyisen työnjaon ja valtionhallinnon tietoturvallisuuden kehittämisen kannalta. Periaatepäätöksessä kuvataan karkealla tasolla VM:n, VAHTIn, Viestintäviraston ja Valtiokonttorin tietoturvatehtäviä. Toimijoiden tehtäviä ei tarkemmin kuvata periaatepäätöksessä, koska työnjakoja ja lainsäädäntöä on tarkoitus kehittää tulevaisuudessa.

Seuraavassa kuvataan nykyinen työnjako ja periaatepäätöksessä mainittujen toimijoiden tehtäviä.

Valtiovarainministeriö

Valtiovarainministeriö vastaa julkishallinnon tietoturvallisuuden ohjauksesta ja kehittämisestä valtioneuvoston ohjesäännön 17 § kohdan 11 mukaisesti. Ohjaus- ja yhteensovittamisroolinsa toteuttamiseksi valtiovarainministeriö asettaa ja ylläpitää toimialallaan yhteistyön ohjaamiseen, kehittämiseen ja koordinaatioon tarvittavat toimielimet.

Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi.

VAHTI

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTIn työn kohteina ovat kaikki tietoturvallisuuden osa-alueet.

VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä. Myös yliopistot ovat aktiivisesti mukana VAHTIn toiminnassa.

VAHTIn toiminnan tuloksia hyödynnetään kansainvälisessä tietoturvatyössä mm. OECD:ssä ja EU:ssa. VAHTIn materiaali on kansainvälisestikin arvioituna korkeatasoista. VAHTI-ohjauksella ja -yhteistyöllä on merkittävästi parannettu valtionhallinnon tietoturvallisuutta. VAHTI-ohjeisto on yksi maailman kattavimmista julkisista tietoturvaohjeistoista.

Liikenne- ja viestintäministeriö

Liikenne- ja viestintäministeriö vastaa viestintäverkkojen ja -palveluiden tietoturvallisuuteen liittyvästä lainsäädännön valmistelusta ja strategia-

työstä. Kansallisella tietoturvastrategialla pyritään edistämään kansalaisten, elinkeinoelämän ja julkishallinnon luottamusta arjen tietoyhteiskunnan palveluiden turvallisuuteen.

Ministeriö on asettanut Arjen tietoyhteiskunnan neuvottelukunnan alaisen arjen tietoyhteiskunnan tietoturvaryhmän, jonka tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi. Ryhmä käsittelee tietoturvallisuuteen liittyviä laajoja ja eri sektoreita ylittäviä kysymyksiä.

Valtioneuvoston asetus liikenne- ja viestintäministeriöstä (405/2003).

Puolustusministeriö

Puolustusministeriö toimii määrättynä turvallisuusviranomaisena (Designated Security Authority; DSA), joka vastaa omalta osaltaan kansainvälisiin sopimuksiin perustuvien turvallisuusluokiteltujen tietojen suojaamista koskevien velvoitteiden toteuttamisesta osana kansallisen turvallisuusviranomaisen (National Security Authority; NSA) kokonaisvastuukenttää.

Puolustusministeriö ohjaa puolustusvoimien DSA-toimien toteuttamista. Puolustusvoimien DSA vastaa tarvittavien yhteisö- ja henkilöturvallisuustodistuksien antamisesta sekä pitää yllä tehtävän edellyttämiä henkilö- ja yhteisöturvallisuusrekistereitä. DSA-tehtävien hoitaminen perustuu lakiin (588/2004) kansainvälisistä tietoturva-velvoitteista.

Puolustusministeriön hallinnonalan tehtävistä on säädetty mm seuraavissa säädöksissä:

- Valtioneuvoston asetus puolustusministeriöstä (375/2003)
- Valtioneuvoston ohjesääntö (262/2003)
- Puolustusministeriön työjärjestys (585/2003)
- Laki puolustusvoimista (551/2007)
- Valtioneuvoston asetuksessa puolustusvoimista (1319/2007).

Ulkoasiainministeriö

Ulkoasiainministeriö toimii kansallisena turvallisuusviranomaisena (National Security Authority, NSA), joka vastaa kansainvälisiin sopimuksiin perustuvien turvallisuusluokiteltujen tietojen suojaamista koskevien velvoitteiden toteuttamisesta. Tehtävän hoitaminen perustuu lakiin (588/2004) kansainvälisistä tietoturvavelvoitteista.

Ulkoasiainministeriön tehtävistä on säädetty ulkoasiainhallintolaissa (204/2000) ja valtioneuvoston asetuksessa ulkoasiainministeriöstä (1171/2005).

Sisäasiainministeriö

Sisäasiainministeriön tehtävänä ovat yleiset tietoturvatehtävät ja ohjeistus silloin, kun ne liittyvät hallinnon verkkoturvallisuuden korkean varautumisen ja tietoturvallisuuden palveluoperaattoripalveluun.

Sisäasiainministeriön tehtävistä on säädetty asetuksella sisäasiainministeriöstä (609/2003) sekä ministeriön työjärjestyksellä (37/2008).

Oikeusministeriö, Tietosuojalautakunta ja Tietosuojavaltuutettu

Oikeusministeriössä on valmisteltu useat hallituksen esitykset, joihin sisältyy tietoturvallisuutta koskevia velvoitteita.

Tietosuojalainsäädännön tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tiedonkäsittelytavan kehittämistä ja noudattamista. Lainsäädännön tavoitteiden toteuttamiseksi henkilötietojen käsittelyä valvoo tietosuojavaltuutettu, joka voi antaa ohjeita henkilörekistereiden suojaamisesta ulkopuoliselta käytöltä. Tietosuoja-asioissa päätösvaltaa käyttää säädetyin tavoin myös tietosuojalautakunta.

Henkilötietolaissa (523/1999) ja luottotietolaissa (527/2007) tarkoitettujen asioiden käsittelemistä varten oikeusministeriön yhteydessä on tietosuojalautakunta ja tietosuojavaltuutetun virka (389/1994).

Ministeriöt hallinnonalallaan

Ministeriöiden velvollisuutena tietoturva- ja varautumisasioissa on aktiivisesti informoida, tulosohjata sekä seurata ja valvoa hallinnonalansa toimenpiteitä. Lisäksi niiden tehtävänä on hallinnonalansa lainsäädännön kehittäminen.

Arkistolaitos

Arkistolaitos antaa arkistolain (831/1994) perusteella asiakirjahallintoon liittyviä määräyksiä ja ohjeita tietoaineistojen säilytyksestä, säilyvyydestä ja hävittämisestä. Lain sähköisestä asioinnista viranomaistoiminnassa (13/2003) nojalla arkistolaitos antaa määräyksiä ja ohjeita sähköisen asioinnin kirjaamisesta tai muusta rekisteröinnistä sekä arkistoinnista.

Huoltovarmuuskeskus

Huoltovarmuuden turvaamisesta annetun lain (1390/1992) tarkoituksena on vakavien häiriöiden ja poikkeusolojen varalta turvata väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömät taloudelliset toiminnot ja niihin liittyvät tekniset järjestelmät eli huoltovarmuus. Tällä lailla on perustettu Huoltovarmuuskeskus, asetettu yleiset tavoitteet ja säädetty sen toiminnan rahoittamisesta.

Valtioneuvosto vahvistaa lain perusteella konkreettiset huoltovarmuuden tavoitteet. Valtioneuvoston päätöksessä (225/2008) määritellään huoltovarmuuden painopistealat ja määrälliset tavoitteet varmuusvarastoinnille ja muille toimenpiteille.

Viestintävirasto

Viestintävirasto toimii kansallisena tietoturvauhkia ja -loukkauksia käsittelevänä CERT-viranomaisena. Tavoitteena on lisätä kansallista ja kansainvälistä tietoturvayhteistyötä sekä kehittää tietoturvauhkiin ja -loukkauksiin liittyviä palveluita helpottamaan organisaatioiden päätöksentekoa. Viestintäviraston tulevana tehtävänä on kehittää tietoliikenteen tietoturvallisuutta (ns. NCSA –toiminta, National Communication Security Authority) kansainvälisten tietoturvavelvoitteiden toteuttamiseksi Suomessa.

Viestintäviraston tehtävistä on säädetty laissa viestintähallinnosta (625/2001) seuraavasti: huolehtia viestintämarkkinalaissa (393/2003), radiolaissa (1015/2001), postipalvelulaissa (313/2001), televisio- ja radiotoiminnasta annetussa laissa (744/1998), valtion televisio- ja radiorahastosta annetussa laissa (745/1998), sähköisen viestinnän tietosuojalaissa (516/2004), eräiden suojauksen purkujärjestelmien kieltämisestä annetussa laissa (1117/2001), sähköisistä allekirjoituksista annetussa laissa (14/2003) sekä verkkotunnuslaissa (228/2003) sille säädetyistä tehtävistä; sekä hoitaa muut tehtävät, jotka sille muiden säännösten tai liikenne- ja viestintäministeriön määräysten mukaan kuuluvat.

Valtion IT-palvelukeskus (VIP)

Vuoden 2009 alusta Valtiokonttorissa toimintansa aloittanut Valtion IT-palvelukeskus toteuttaa osaltaan valtion IT-strategiaa valtion IT-toiminnan johtamisyksikön ohjauksessa sekä vastaa valtion IT-strategian mukaisten yhteisten tai yhtenäistettyjen IT-palvelujen tuotannon järjestämisestä. Valtionhallintotason tietoturvapalvelut ovat keskeinen osa VIPin toimintaa.

Valtion IT-palvelukeskuksen tehtävät on määrätty valtioneuvoston asetuksessa valtiokonttorista (1155/2002) ja asetuksen muutoksessa (844/2008).

Hallinnon tietotekniikkakeskus (HALTIK)

Sisäasiainministeriön Hallinnon tietotekniikkakeskuksen tehtävänä on tuottaa hallinnon verkkoturvallisuuden korkean varautumisen ja tietoturvallisuuden palveluoperaattoripalvelut turvallisuusviranomaisille kaikissa turvallisuustilanteissa. Tietotekniikkakeskus vastaa sisäasiainministeriön hallinnonalalla tietoteknisten peruspalvelujen, tietotekniikkaan liittyvien asiantuntijapalvelujen sekä turvaklusteripalvelujen tuottamisesta tilaaja-tuottaja -periaatteella. Keskus tuottaa palveluita myös muille valtion virastoille ja laitoksille palvelusopimusten perusteella.

Toiminnan perustana on valtioneuvoston asetus (810/2007) hallinnon tietotekniikkakeskuksesta ja laki poliisin hallinnosta (110/1992).

Puolustusvoimien johtamisjärjestelmäkeskus (PVJJK)

Puolustusvoimien johtamisjärjestelmäkeskus on korkeassa valmiudessa oleva verkko- ja palveluoperaattori, joka mahdollistaa puolustusvoimien tiedustelun, valvonnan ja johtamisen kaikissa turvallisuustilanteissa. Lisäksi se kehittää ja tuottaa tietohallinnon palveluita koko puolustushallinnolle sekä soveltuvin osin laajemmin julkishallinnolle ja puolustushallinnon yrityskumppaneille sekä tarjoaa kansallisesti ja kansainvälisesti muualla valtionhallinnossa ja yrityksessä kehitettyjä tietohallinnon palveluita soveltuvin osin koko puolustushallinnon käyttöön.

Keskus tuottaa hallinnonalan verkkoturvallisuuden korkean varautumisen ja tietoturvallisuuden verkko-operaattoripalvelut turvallisuusviranomaisille kaikissa turvatilanteissa.

Poliisiviranomaiset

Poliisiviranomaiset suorittavat tietotekniikkarikollisuuden ennaltaehkäisemistä, selvittämistä ja syyteharkintaan saattamista. Laki poliisin hallinnosta (110/1992).

Suojelupoliisi ja paikallispoliisi toimivat lausunnon antajana henkilöstöturvallisuusselvityksissä. Laki turvallisuusselvityksistä (177/2002).

Hallinnonalakohtaiset tietoturvatoimijat

Eräillä muilla hallinnonaloilla on organisaatioita, jotka tarjoavat tietoturva- ja tietotekniikkapalveluita omalle hallinnonalalleen.

5 Toimeenpano ja resurssit

Jokaisella viranomaisella on omalta osaltaan vastuu tietoturvallisuuden johtamisesta ja jalkautustoimista osaksi organisaation turvallisuustoimintoja ja toiminnan prosesseja. Tietoturvallisuuden ohjaus ja kehittäminen hoidetaan aluksi olemassa olevissa ja tulevaisuudessa tarvittavin osin uusittavissa organisaatiorakenteissa. Merkittäviä uudistuksia tarvitaan luvun 3 kehittämisperiaatteiden, painopisteiden ja kehittämiskohteiden jalkauttamiseksi.

Periaatepäätöksen toteuttamiseksi ja tietoturvatyön tehostamiseksi viranomaiset toteuttavat ja resursoivat valtion tietoturvallisuuden kehittämisohjelman vuosille 2010 – 2015. Kehittämisohjelman tavoitteena on taata riittävän hyvän tietoturvallisuuden varmistaminen, tietoturvariskien hallinta, ICT-varautumisen parantaminen, tietoturvallisuuden integroituminen hallinnon toimintaan, yhteistyön edelleen kehittäminen sekä mahdollisten uusien katvealueiden toteaminen ja hallinta. Kehitysohjelman valmistelu on jo käynnissä VAHTIssa. Valtionhallintotason tietoturvallisuuden kehitysohjelma on edellytys hallinnon toiminnan johtamiselle, laadulle, osaamiselle, jatkuvuudelle ja varautumiselle. Edellisellä, vuosien 2004 – 2006 kehitysohjelmalla parannettiin merkittävästi valtion tietoturvallisuutta.

Valtiohallintotasoisen tietoturvayhteistyön vahvistaminen tarkoittaa eri organisaatioiden asiantuntijoiden aktiivista osallistumista kehittämiseen ja toimeenpanoon liittyvään valtionhallintotason työhön. Tämän voidaan arvioida tarkoittavan noin 200 asiantuntijan osalta keskimäärin 10 – 15 htp vuosittaista panosta oman virkatyönsä ohessa valtiohallintotasoiseen tietoturvatyöhön. Yhteistyön tuottama henkilötason verkosto edistää hyvien käytäntöjen käyttöönottoja sekä kehittää turvallisuuskulttuuria kustannustehokkaasti.

6 Seuranta ja raportointi

Raportointi ja valvonta ovat osa tulosohjauksen keinovalikoimaa. Tulosohjausmallin mukaisesti jokainen ministeriö asettaa tietoturvatavoitteet hal-

linnonalansa virastoille tulosohjauksessa sekä valvoo toimialansa virastojen toimintaa saamiensa raporttien avulla. Valtiovarainministeriö kehittää seurantaa osana konserniohjausta. Valtiontalouden tarkastusvirastolla ja Tietosuojavaltuutetulla on oman toimialansa osalta säädösperustaiset oikeudet saada tietoa valtionhallinnosta.

Talousarvioasetuksen 65 § ja 69 §:ssä on todettu, että viraston johdon tulee vuosittain antaa lausuma organisaationsa riskienhallinnan tilasta osana viraston tilinpäätöstietoja. Lausuma edellyttää, että organisaatiossa on olemassa dokumentoitu, johdon hyväksymä riskienhallintapolitiikka ja siihen liittyvä säännöllinen raportointi johdolle.

Valtiontalouden tarkastusviraston tehtävänä on tarkastaa valtion taloudenhoidon laillisuutta ja tarkoituksenmukaisuutta sekä valtion talousarvion noudattamista. Tässä näkökulmassa tarkastus kohdistuu mm. talousarvioasetuksen 65 § ja 69 § noudattamiseen. Laki valtiontalouden tarkastusvirastosta (676/2000). Tarkastusvirasto päättää itse toimintansa kohteet.

7 Periaatepäätöksen vaikutukset

Esitetyt toimet tehdään toiminnan taloudellisten kehysten ja vuosittain talousarvion yhteydessä tehtävien päätösten puitteissa. Valtionhallinnon toiminnan laatu, riskien hallinta ja jatkuvuus edellyttävät hallinnonaloilla ja virastoissa resurssien priorisointia tietoturvallisuuden ja varautumisen kannalta keskeisiin kohteisiin.

Esityksellä on valtiontaloudellisia vaikutuksia, jotka aiheutuvat valmisteltavasta ja toteutettavasta valtion tietoturvallisuuden kehittämisohjelmasta sekä periaatepäätöksen linjausten toimeenpanosta hallinnon toiminnassa ja hankkeissa. Taloudellisten vaikutusten suuruus tarkastellaan hankekohtaisesti toimeenpanon yhteydessä.

Periaatepäätös edellyttää johtamisen ja osaamisen kehittämistoimenpiteitä. Suuressa osassa toimijoita tulee vahvistaa tietoturvallisuuden ja varautumisen sisällyttämistä toiminnan ja talouden suunnitteluun sekä johtamiseen ja tulosohjaukseen.

8 Voimaantulo

Tarkoitus on, että tämä periaatepäätös tulisi voimaan 1. päivänä joulukuuta 2009 ja sillä kumottaisiin valtioneuvoston 11.11.1999 antama periaatepäätös valtionhallinnon tietoturvallisuudesta (VM 0024:00/02/99/1998).

Voimassaolevat VAHTI-julkaisut

VAHTI 7/2009 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009 Kohdistetut hyökkäykset
VAHTI 5/2009 Effective Information Security
VAHTI 4/2009 Information Security Instructions for Personnel
VAHTI 3/2009 Lokiohje
VAHTI 2/2009 ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin
VAHTI 1/2009 VAHTIn toimintakertomus vuodelta 2008
VAHTI 9/2008 Hankkeen tietoturvaohje
VAHTI 8/2008 Valtionhallinnon tietoturvasanasto
VAHTI 7/2008 Informationssäkerhetsanvisningar för personalen
VAHTI 6/2008 Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista
VAHTI 5/2008 Valtion ympärivuorokautisen tietoturvavalvonnan hankeesitys
VAHTI 4/2008 Valtionhallinnon tietoturva-arviointipoolin toimintaraportti
VAHTI 3/2008 Salauskäytäntöjä koskeva tietoturvaohje
VAHTI 2/2008 Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 1/2008 Toimintakertomus 2007
VAHTI 3/2007 Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 2/2007 Älypuhelinten tietoturvallisuus
VAHTI 1/2007 Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006 Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006 Tietoturvakouluttajan opas
VAHTI 10/2006 Henkilöstön tietoturvaohje

VAHTI 9/2006 Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006 Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006 Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje
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 5/2003 Datasäkerhetsanvisning för användaren
VAHTI 5/2003 User´s Information Security Instruction
VAHTI 3/2003 Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003 Turvallinen etäkäyttö turvattomista verkoista
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 2/2001 Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 3/2000 Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000 Valtion tietoaineistojen käsittelyn tietoturvaohje

Ohjeisto löytyy VAHTIn verkkosivuilta www.vm.fi/vahti -> voimassa olevat VAHTI-ohjeet. Samalla sivulla on myös tietoa ohjeiden tilaamisesta painotalo Editasta. VAHTIn verkkosivuilta löytyy myös VAHTIn toiminnasta kertovia raportteja.

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

7/2009
VAHTI
marraskuu 2009

ISSN 1455-7606 (nid.)
ISBN 978-952-251- 016-7 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-017-4 (pdf)