VALTIOVARAINMINISTERIÖ

VAHTI

VAHTI:n toimintakertomus vuodelta 2015

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
– VAHTI 1/2016

Julkisen hallinnon ICT

VALTIOVARAINMINISTERIÖ

VAHTI:n toimintakertomus vuodelta 2015

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
– VAHTI 1/2016

Julkisen hallinnon ICT

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Valtioneuvoston hallintoyksikkö/Tietotuki- ja julkaisuyksikkö / Pirkko Ala-Marttila

ISSN 1798-0860 (pdf)
ISBN 978-952-251-760-0 (pdf)

Johdanto

Hyvin toteutettu tieto- ja kyberturvallisuus on yhteiskunnan toimivuuden edellytys kaikissa olosuhteissa. Tieto- ja kyberturvallisuus on olennainen osa hallinnon toimintaa ja riskien hallintaa sekä toiminnan luotettavuuden, laadun, jatkuvuuden ja sujuvuuden varmistamista. Kokonaisuuden avulla voidaan varmistaa menestyksekäs, tavoitteiden mukainen toiminta. Tieto- ja kyberturvallisuus tulisi nähdä toiminnan mahdollistaja, joka myös mahdollistaa uudet, digitalisoidut, automatisoidut prosessit ja palvelut.

Valtiovarainministeriössä (VM) julkisen hallinnon ICT:n ohjauksesta ja kehittämisestä vastaavana organisaationa on Julkisen hallinnon tieto- ja viestintätekninen osasto (JulkICT), joka toimii ministeriön ylimmän johdon alaisuudessa. Laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011) korostaa valtiovarainministeriön roolia ja vastuuta koko julkisen hallinnon ICT:n ohjaajana.

Valtiovarainministeriö vastaa julkisen hallinnon tietoturvallisuuden yleisestä kehittämisestä ja valtionhallinnon tietoturvallisuuden ohjauksesta. Ministeriö on asettanut Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) hallinnon tieto- ja kyberturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI käsittelee kaikki merkittävät valtionhallinnon kyberturvallisuuden ja tietoturvallisuuden linjaukset. VAHTIssa ovat edustettuina eri hallinnonalat ja -tasot sekä kunnat.

VAHTIn toiminnalla parannetaan valtion tieto- ja kyberturvallisuutta, ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Toiminnan tuloksena on saatu aikaan kattava yleinen tietoturvaohjeisto (http://www.vahtiohje.fi). VM:n ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen yhteisiä, tietoturvallisuutta parantavia hankkeita. Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä.

VAHTIn toiminnan tuloksia hyödynnetään kansainvälisessä tieto- ja kyberturvatyössä mm. OECD:ssä. VAHTIn materiaali on myös kansainvälisesti arvioituna korkeatasoista.

Tässä julkaisussa kuvataan VAHTIn toimintaa, yhteistyötä ja vaikuttavuutta vuonna 2015. Julkaisun luvuissa 4 ja 11 kuvataan valtionhallinnon tieto- ja kyberturvallisuuden kehitystä ja tilannetta 2015 VAHTIn mittareilla arvioituna. Kokonaisuutena valtionhallinnon tieto- ja kyberturvallisuus pysyi pääosin samalla tasolla edelliseen vuoteen nähden; osa seurattavista mittareista laski aavistuksen verran, osa säilyi samalla tasolla, yksittäisissä osa-alueissa tapahtui edistymistä. Tämän onnistumisen yksi perusta on ollut valtiovarainministeriön ohjaus, kehittäminen ja laaja-alainen yhteistyö.

Inledning

Välskött informations- och cybersäkerhet är under alla förhållanden en förutsättning för att samhället ska fungera. Informations- och cybersäkerheten är en väsentlig del av förvaltningens verksamhet och riskhantering samt säkerställandet av verksamhetens pålitlighet, kvalitet, kontinuitet och smidighet. Med hjälp av helheten kan man säkerställa framgångsrik verksamhet som är förenlig med målsättningarna. Informations- och cybersäkerheten borde också ses som möjliggörare av verksamheten, med vars hjälp man kan tillhandahålla nya digitaliserade, automatiserade processer och tjänster.

Den offentliga förvaltningens informations- och kommunikationstekniska funktion (JulkICT), som agerar direkt under ministeriets högsta ledning, är det organ inom finansministeriet som svarar för styrningen och utvecklingen av IKT inom den offentliga förvaltningen. Den nya lagen om styrning av informationsförvaltningen inom den offentliga förvaltningen (634/2011) framhäver finansministeriets roll och ansvar vid styrningen av hela den offentliga förvaltningens ICT.

Finansministeriet (FM) svarar för den allmänna utvecklingen av informationssäkerheten inom den offentliga förvaltningen samt för styrningen av informationssäkerheten inom statsförvaltningen. Ministeriet har tillsatt Ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen (VAHTI) som ett organ för samarbete, styrning och utveckling av informationssäkerheten inom förvaltningen. VAHTI behandlar alla viktiga riktlinjer för informations- och cybersäkerheten inom statsförvaltningen. Olika förvaltningsområden och –nivåer är representerade i VAHTI.

VAHTI förbättrar statens datasäkerhet, och arbetet påverkar inte bara förvaltningen utan även företag och internationella aktörer. Verksamheten har resulterat i en täckande allmän datasäkerhetsanvisning (www.vm.fi/vahti och http://www.vahtiohje.fi). Ministerierna och ämbetsverken har under finansministeriets och VAHTIs ledning genomfört flera framgångsrika gemensamma projekt som förbättrat informationssäkerheten. Resultaten av VAHTIs verksamhet utnyttjas utöver statsförvaltningen även inom kommunförvaltningen, den privata sektorn, medborgarverksamheten och det internationella samarbetet.

Resultaten av VAHTIs verksamhet utnyttjas inom internationellt informations- och cybersäkerhetssamarbete bl.a. av OECD. VAHTIs material håller hög standard även i internationell jämförelse.

Denna publikation beskriver VAHTIs verksamhet, samarbete och inverkan år 2015. I kapitlen 4 och 11 beskrivs utvecklingen av informations- och cybersäkerheten inom statsförvaltningen samt läget 2015, enligt VAHTIs mätare. Informations- och cybersäkerheten

inom statsförvaltningen hölls i det stora hela både ur övergripande perspektiv och enligt flera mätare på samma nivå som 2015. En del av referensvärdena sjönk aningen, en del hölls på samma nivå och enstaka delområden uppvisade utveckling.

Styrningen, utvecklandet och det omfattande samarbete som finansministeriets utför har varit en grundläggande faktor som bidrar till framgången.

Introduction

Well-managed information and cyber security is a precondition for the functioning of society in all circumstances. Information and cyber security is an essential part of effective administration and risk management. It also helps to ensure the reliability, quality, continuity and smooth operation of public services. These matters must be in place to ensure successful, goal-oriented activities. Information and cyber security should be considered as an enabler, which facilitates the introduction of new, digitalised and automated processes and services.

The Public Sector ICT department (JulkICT) operating directly under senior leadership of the Ministry of Finance is responsible for the guidance and development of public administration ICT. The act on information management guidance in public administration (Laki julkisen hallinnon tietohallinnon ohjauksesta 634/2011) underscores the role and responsibility of the Ministry of Finance for steering ICT operations in the whole public sector.

The Ministry of Finance is responsible for the overall development of information security in public administration and the guidance of information security in central government. The Ministry has appointed the Government Information and Cyber Security Management Board (VAHTI) to supervise the cooperation, steering and development of central government information and cyber security. VAHTI provides all the main policy guidelines for information and cyber security in central government. Different administrative branches and levels of central administration and local government are represented in VAHTI.

VAHTI improves Government information and cyber security, and the effectiveness of the work can be seen not only in the administration but also on an international scale. The outcome is a set of general information security instructions (http://www.vahtiohje.fi). Several joint information security projects launched by the ministries and government agencies have been successfully implemented under the direction of the Ministry of Finance and VAHTI. VAHTI guidelines and instructions are also useful for local authorities, the private sector, civil society and international cooperation.

The results of the work are used in international information and cyber security forums such as the OECD. VAHTI publications are considered to be of high quality by international standards.

This publication describes the operation, cooperation and effects of VAHTI in 2015. Chapters 4 and 11 of the publication describe the development and situation of central government information and cyber security in 2015. On the whole, central government information and cyber security was as good as before; some of the indicators dropped slightly, some remained at the same level, and improvement took place in the context of certain indicators. The good results are partly based on steering, development and cooperation within Ministry of Finance.

Sisältö

1 VAHTIn tieto- ja kyberturvallisuuden kehittämisalueet 2015

VAHTIn toiminnassa on vuonna 2015 pyritty edelleen tietoturva- ja kyberturvatyön vaikuttavuuden parantamiseen sekä käsitelty myös tietosuojaan liittyviä asioita. Vuoden aikana on perustettu ja käynnistetty uusi VAHTIn kuntien tietoturvajaosto sekä päätetty asettaa työryhmä selvittämään EU-tietosuojalainsäädännön muutosten vaikutuksia. VAHTIn ohjejaosto on käynnistänyt kolme uutta ohjehanketta sekä erillisen kehittämishankkeen koko ohje- ja vaatimuskokonaisuuden uusimiseksi. VAHTI-johtoryhmä on ohjannut, koordinoinut ja sovittanut yhteen laaja-alaisesti valtion tieto- ja kyberturvallisuuden kokonaisuutta sekä hankkeita.

Seuraavissa kappaleissa kuvataan lyhyesti toimenpiteiden ja hankkeiden painopisteitä hyödyntäen valtionhallinnossa yleisesti käytettävää CAF-laatuarviointimallia, johon myös tietoturvatasojen vaatimukset kytkeytyvät.

Hankkeiden tilannetta 31.12.2015 on kuvattu liitteessä 4.

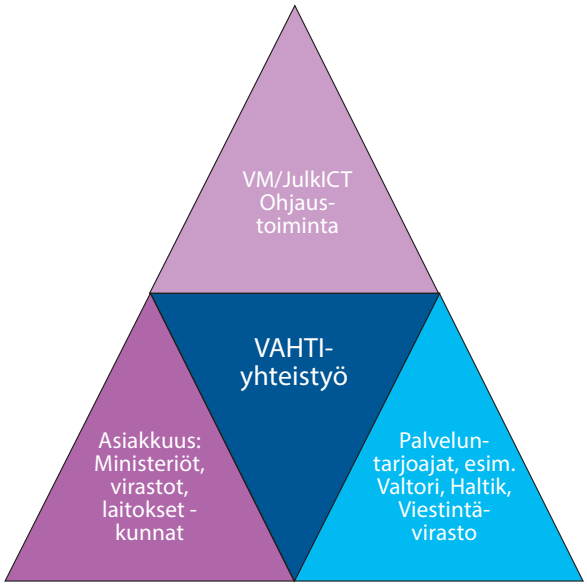
Johtajuus

VAHTI on tukenut tieto- ja kyberturvallisuuden liittämistä hallinnon johtamiseen ja kehittämiseen sekä tieto- ja kyberturvallisuuden johtamista käynnistämällä, toimeenpanemalla ja ohjaamalla hankkeita, joilla tuetaan periaatepäätöstä valtionhallinnon tietoturvallisuuden kehittämisestä sekä tietoturvallisuusasetuksen toimeenpanoa. VAHTI on asettanut Valtion tieto- ja viestintätekniikkakeskus Valtorin toteuttamaan korotetun tietoturvatason ja ICT-varautumisen yhteishankkeen. Yhteishankkeen avulla on tuettu korotetun tietoturvatason vaatimusten soveltamista valtionhallinnon viranomaisten tuottamissa palveluissa.

JulkICT-toiminto ja VAHTI ovat ohjanneet ja rahoittaneet mm. Valtorin ja Viestintäviraston toteuttamia tietoturvapalveluita viranomaisille.

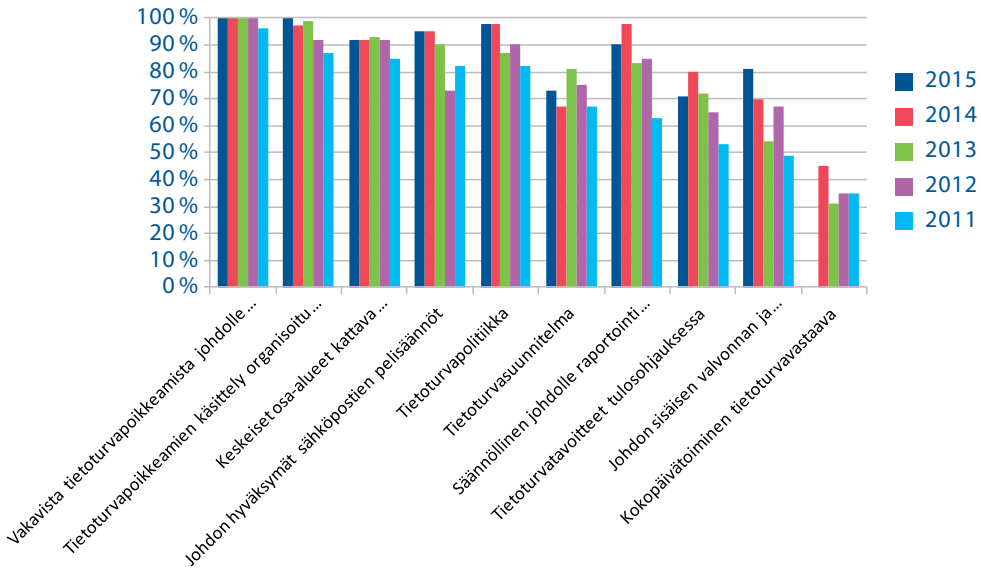
Oheisessa kaaviossa on esitetty valtionhallinnon tieto- ja kyberturvallisuuden johtamisen ja yhteistyön malli.

Kuva 1. Tieto- ja kyberturvallisuuden ohjausmalli



Tieto- ja kyberturvallisuuden johtamisen arvioimiseksi on kehitetty VAHTIssa useita mittareita, joita on käytetty VAHTI-kyselyssä osin jo vuodesta 2009 saakka.

Kuva 2. Tietoturvallisuuden johtamisen mittareita. Kuvassa esitetään tietoturvallisuuden johtamiseen liittyvien mittarien kehitys vuosina 2011-2015 organisaatioiden oman arvion mukaan. Koska johtaminen on hyvin keskeinen osa-alue, sen seurannassa käytetään kymmentä VAHTIn mittaria.



Kyselyyn vastasi 61 kaikkiaan viranomaista. Vastaavaan kunnille lähetettyyn kyselyyn vastasi 93 kuntaa tai kaupunkia.

Kehitys on ollut merkittävää vuoteen 2014 asti, jonka jälkeen mittareissa on nähtävissä pienempiä muutoksia. Kokonaisuutena johtajuuden mittareiden keskiarvo on pysynyt samalla tasolla vuosina 2014–2015. Nyt kaksi osa-aluetta on 100 prosenttia: ”Vakavista tietoturvapoikkeamista johdolle raportointi” sekä uutena kohtana ”Tietoturvapoikkeamien käsittely organisoitu / vastuutettu”.

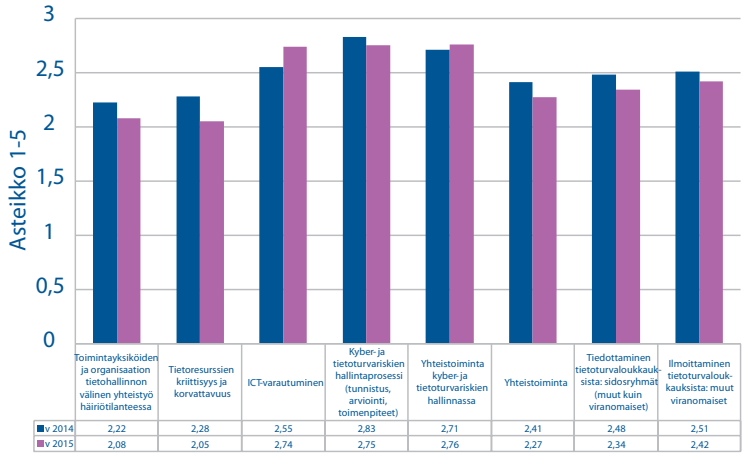
Parhaiten kehittynyt osa-alue oli ”Johdon sisäisen valvonnan ja riskienhallinnan arviointi- ja vahvistuslausumassa käsitellään tietoturvariskejä”, joka nousi vuodessa 70 prosentista 81 prosenttiin. Vastaavasti eniten laskenut osa-alue oli ”Tietoturvatavoitteet tulosohjauksessa”, joka on laskenut 80 prosentista 71 prosenttiin.

Strategiat ja toiminnan tukeminen

Tietoturvallisuusasetuksen mukaista toimintaa tuetaan kehittämällä edelleen VAHTI-ohjeistoa. Erityisesti tietoturvatasojen ja ICT-varautumisen vaatimukset sekä niiden toimeenpanoa tukevat ohjeet auttavat viranomaisia tietoturvaresurssien tarkoituksenmukaisessa kohdentamisessa. VAHTI käynnisti vuonna 2015 erillisen hankkeen ohjeiston rakenteen uudistamiseksi ja ohjeiston ylläpidettävyyden parantamiseksi. Samassa yhteydessä käydään läpi olemassa olevat tietoturvavaatimukset sekä laaditaan niistä oma erillinen vaatimuskokonaisuutensa, joka irrotetaan VAHTI-ohjeista.

Suomen kyberturvallisuusstrategia (2013) korostaa VAHTIn roolia ja vastuuta julkisen hallinnon tieto- ja kyberturvallisuuden yhteistyön ja kehittämisen toimielimenä. VAHTIssa toimivat organisaatiot ovat keskeisessä roolissa strategian toimeenpanossa ja yhteistyössä. VAHTI on aktiivisesti seurannut kyberturvallisuusstrategian toimeenpanoa eri hallinnonaloilla.

Kuva 3. Kyberturvallisuuden kypsyystaso. Kuvassa VAHTI-kyselyn kahdeksan kyberturvallisuuden osa-alueen tulokset vuosilta 2014-2015.



Kahdeksasta osa-alueesta kuusi laski hieman, vastaavasti kaksi osa-aluetta nousi. Keskiarvo laski hieman eli 2,50 pisteestä 2,43 pisteeseen. Maksimipistemäärä tässä kypsyystason arvioinnissa on viisi ja minimi on yksi. Näiden osa-alueiden osalta vahvuudet ovat ”Yhteistoiminta kyber- ja tietoturvariskien hallinnassa (2,76)”, ”kyber- ja tietoturvariskien hallintaprosessi” (2,75) sekä ”ICT-varautuminen (2,74)”.

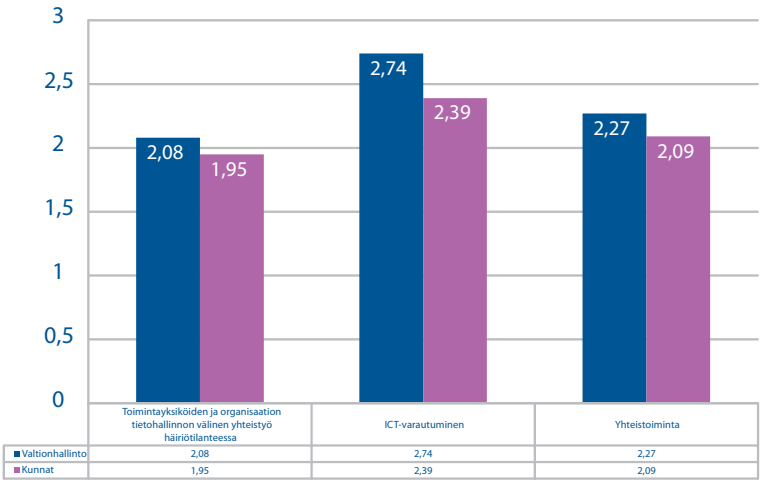
Eniten kehittämistä vaativia osa-alueita ovat ”Tietoresurssien kriittisyys ja korvattavuus” (2,05), ”Toimintayksiköiden ja organisaation tietohallinnon (tai vastaavan) välinen yhteistyö häiriötilanteessa” (2,08) sekä ”Yhteistoiminta” (2,27).

Osana VAHTIn toimeenpanoa on todettu tarve entistä vahvemmin kehittää kuntien tietoturvallisuutta ja hyödyntää tässä VAHTIa ja sen tuloksia. Tämän tavoitteen toteuttamiseksi valtiovarainministeriö asetti vuonna 2015 kuntien tietoturvallisuutta kehittävän VAHTI-jaoston. Vuonna 2015 toteutettiin vastaavanlainen kysely kuntien tieto- ja kyberturvallisuuden nykytilanteesta.

Kuntien kyberturvallisuudesta mitattiin kolmen osa-alueen avulla:

1. Toimintayksiköiden ja organisaation tietohallinnon (tai vastaavan) välinen yhteistyö häiriötilanteessa
2. ICT-varautuminen
3. Yhteistoiminta

Kuva 4. Kyberturvallisuuden kypsyystaso valtionhallinnossa ja kunnissa. Vuonna 2015 kuntien tietoturva- ja kyberturvallisuuskyselyssä kysyttiin kolmesta osa-alueesta. Ero valtionhallinnon ja kuntien välillä on suurin ICT-varautumisessa, jota VAHTI on määrätietoisesti kehittänyt valtionhallinnossa vuodesta 2009 saakka.



VAHTI käynnisti vuonna 2015 hankkeen, joka ohjeistaa viranomaisia toiminnan jatkuvuuden turvaamisessa ja jatkuvuustoiminnan ohjaamisessa.

Henkilöstö

VAHTIssa on linjattu, että henkilöstön tietoturva-, kyberturvallisuus- ja ICT-varautumisen tietoisuutta ja osaamista tulee vahvistaa.

Valtorin tuottama työkalupakki ja verkkokoulutukset

Valtori tukee tietoturvavastaavien työtä ylläpitämällä sähköistä työkalupakkia, joka sisältää materiaaleja ja mallipohjia valtionhallinnon tietoturvallisuudesta vastaaville henkilöille. Työkalujen sisältö perustuu VAHTIn ohjeisiin. Materiaalia hyödynnetään kaikissa virastoissa.

Työkalupakki sisältää myös Moodle-pohjaisen verkkokoulutusympäristön. Tarjolla ovat seuraavat koulutusaineistot:

- Henkilöstön tietoturvakurssi (Vahti 4/2013)
- Johdon tietoturvakoulutus (Vahti 2/2011)
- ICT-varautuminen (Vahti 2/2012)
- ICT-hankintojen tietoturvakoulutus (Vahti 3/2011)
- Sosiaalisen median tietoturvakurssi (Vahti 4/2010)
- Tietoaineiston käsittelykurssi

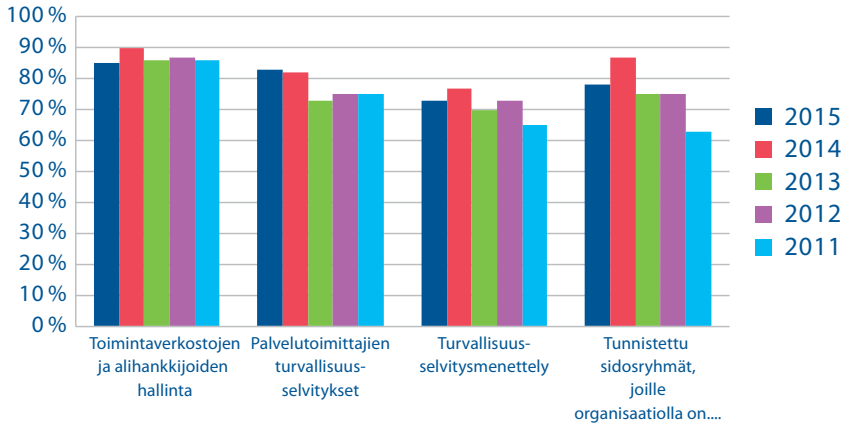
Moodlessa on kaikkiaan 18 334 käyttäjää 54 valtionhallinnon organisaatiosta, käytössä on 127 eri kurssia eli 2,35 kurssia / organisaatio. Työkalupakin käyttö on maksutonta.

Kumppanuudet ja resurssit

VAHTI on tukenut kumppanuuksien kehittämistä vuonna 2015 toimenpiteillä tietotekniikkahankintojen tietoturvaohjeen jalkauttamiseksi. Ohjeen liitteinä olevaa turvallisuussopimusmallia on päivitetty ja uusi sopimusmalli otetaan käyttöön vuonna 2016. Vuonna 2015 julkaistiin sivustolla www.vahtiohje.fi uusi tukimateriaali ”12 Liite 5. Tietoturvallisuuden ja jatkuvuudenhallinnan huomioiminen hankittaessa ulkoistettuja ICT-palveluita”.

VAHTI toimii jatkuvassa ja tiiviissä yhteistyössä puolustusministeriön yhteydessä toimivan Turvallisuuskomitean ja muiden turvallisuusviranomaisten, kuten kansainvälisistä tietoturvavelvoitteista vastaavan ulkoasiainministeriön kansallisen turvallisuusviranomaisen ja Viestintäviraston Kyberturvallisuuskeskuksen kanssa. Niiden toimintaa on käsitelty säännöllisesti VAHTIn kokouksissa.

Kuva 5. Kumppanuuksien hallinnan mittarit. Kuvassa esitetään seurattavien kohteiden toimeenpano valtionhallinnon organisaatioissa vuosina 2011 - 2015.



Neljästä osa-alueesta kolme on laskenut ja yksi on noussut, ”Palvelutoimittajien turvallisuusselvitykset”. Osa-alueen keskiarvo on laskenut 84 prosentista 79 prosenttiin. Eräs keskeinen syy tähän liittyy useampaan viime vuoden aikana liikkeelle lähteneeseen tai edelleen vaikuttavaan valtionhallinnon ICT-palvelutuotantoon liittyvään muutokseen, esimerkiksi Valtorin käynnistymiseen sekä Valtioneuvoston hallintoyksikön perustamiseen.

Valtorin tuottama tietoturvallisuuden asiantuntijapalvelu

Valtori käynnisti valtiovarainministeriön JulkICT-toiminnon toimeksiannosta maaliskuussa 2014 Hanselin johdon puitejärjestelyn avulla toteutetun tietoturvallisuuden asiantuntijapalvelun. Valtorin asiakkaat voivat tilata tätä kautta tieto- ja kyberturvallisuutta, tietosuojaa tai jatkuvuuden hallintaa ja varautumista edistäviä toimeksiantoja. Toimeksiannot voivat koostua esimerkiksi konsultoinnista, koulutuksesta, teknistä tietoturvallisuutta edistävistä toimeksiannoista tai konsulttien suorittamista katselmoinneista ja auditoinneista. Palvelu pohjautuu Valtion IT-palvelukeskuksen vuonna 2010 kehittämään vastaavaan palveluun. Palveluiden kautta on tilattu toimeksiantoja seuraavasti:

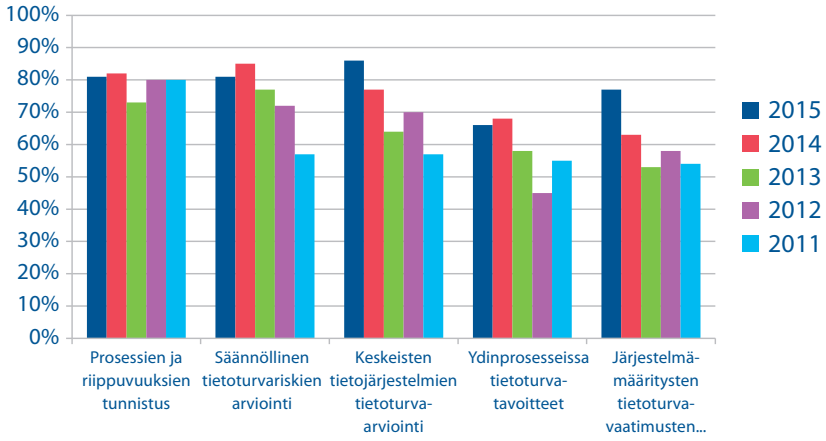
vuosi	toimeksiantojen lkm	htp
2015	144	4 194
2014	101	2 812
2013	135	2 576
2012	103	2 491
2011	72	1 130
2010	63	1 091

Toiminnan prosessit

Tietoturvallisuuden hallintajärjestelmien arvioinnit ovat jatkuneet Tietoturvallisuusasetuksen 5 § perustason saavuttamisen todentamiseksi. Tekniset tietoturva-arvioinnit ovat vakiintuneet entistä laajemmin osaksi uusien tietojärjestelmien ja -palveluiden käyttöönottoa. VM:n pyynnöstä on tehty arviointeja tietoturvallisuuden arviointilain (1406/2011) 5 § perusteella.

VAHTI käynnisti ohjehankkeet, joilla viranomaisia ohjeistetaan tietoturvapoikkeamien hallinnassa sekä sähköisen asioinnin tietoturvallisuuden kehittämisessä. Ohjeet valmistuvat vuoden 2016 aikana.

Kuva 6. Toiminnan prosessien mittarit. Kuvassa esitetään tietoturvallisuuden prosessien toimeenpano vuosina 2011–2015.



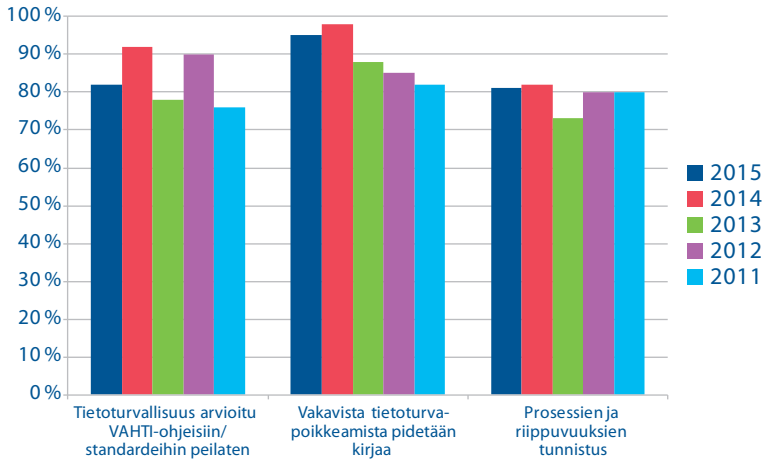
Pitkällä aikavälillä tilanne on parantunut hyvin kaikilla osa-alueilla, erityisesti auditoinneissa parannus on ollut merkittävää. Viidestä osa-alueesta kolme laski lievästi, mutta ”Keskeisten tietojärjestelmien tietoturva-arviointi” nousi 77 prosentista 86 prosenttiin sekä ”Järjestelmämääritysten tietoturvavaatimusten auditointi” on noussut 63 prosentista 77 prosenttiin. Kokonaisuutena osa-alueen keskiarvo on noussut 75 prosentista 78 prosenttiin.

Mittaaminen

Mittaaminen on keskeinen osa tietoturvallisuuden ohjausta. VAHTIn mittaristoa ja mittaamista pyritään jatkuvasti kehittämään. VAHTIn vuosittaista valtionhallinnon tietoturvakyselyä tarkennettiin edelleen, jotta sen avulla saataisiin tarkempaa seurantatietoa sekä viranomaisille palautetta niiden omasta tietoturvallisuuden tasosta. Kyselyyn vastasivat ministeriöt sekä suurin osa virastoista (kaikkiaan 61 vastausta, vastausmäärä on hieman noussut viime vuosina).

VAHTI on käsitellyt ja asettanut tärkeysjärjestykseen Viestintävirastolle osoitettavia verkkojen ja tietojärjestelmien turvallisuuden arvioinnin tehtäviä lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) perusteella. Arviointitoimintaa on tuettu vuonna 2014 julkaistulla tietoturvallisuuden arviointiohjeella. Tätä tarkennetaan teknisen jaoston valmistelussa olevalla ohjeella auditointiin valmistuvalle organisaatiolle ja sitä toteuttaville toimittajille vuonna 2016.

Kuva 7. Mittaaminen. Kuvassa esitetään tietoturvallisuuden mittaamisen tilannetta vuosina 2011–2015.



Mittareissa ei ole tapahtunut suurta muutosta edelliseen vuoteen verrattuna, tosin kaikki kolme osa-aluetta ovat laskeneet, eniten ”Tietoturvallisuus arvioitu VAHTI-ohjeisiin/ standardeihin peilaten”. Tätä voidaan perustella sillä, että organisaatioilla on ollut tarve saavuttaa organisaation tietoturvallisuuden perustaso vuonna 2013, minkä jälkeen tälle arvioinnille ei ole ollut enää niin suurta vuosittaista tarvetta.

2 VAHTIn tavoitteet ja tehtävät

Valtiovarainministeriö on asettanut Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) hallinnon tieto- ja kyberturvallisuuden yhteistyön, ohjauksen ja kehittämisen toimielimeksi.

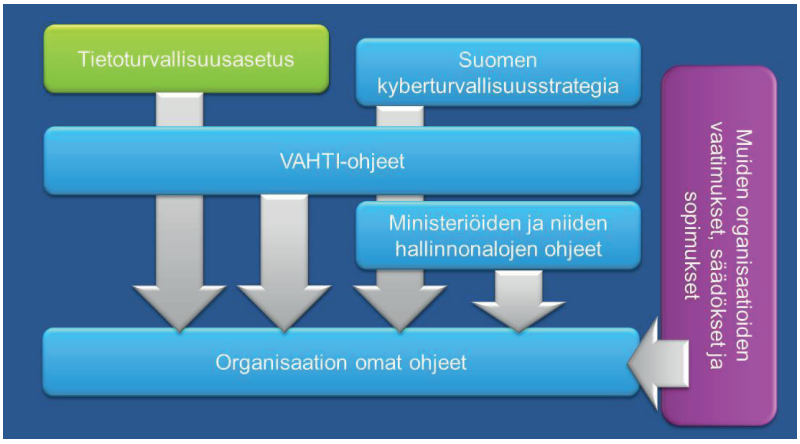
Tieto- ja kyberturvallisuuden ohjauksesta ei ole Suomessa kattavaa lainsäädäntöä. Tässä hajautetussa työnjaossa VAHTIn merkitys yhteistyön sekä tieto- ja kyberturvallisuuden kehittämisen tehostajana on korostunut.

VAHTIn tavoitteena on parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tieto- ja kyberturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. VAHTIlla on keskeinen rooli myös valtion ICT-toimintojen ohjauksessa.

VAHTIn tehtäviä on kuvattu tarkemmin VAHTIn sivuilla www.vm.fi/vahti sekä VAHTI-johtoryhmän asettamispäätöksessä.

VAHTIn toiminnan yksi keskeinen alue on valtionhallinnon yhteisten tieto- ja kyberturvallisuuslinjausten valmistelun ohjaus, käsittely ja hyväksyntä. Organisaatioiden pääsääntönä tulee olla valtionhallintotason VAHTI-linjausten mukainen toiminta. Kuva 8 esittää yksinkertaistetusti tietoturvallisuuden normistoa valtionhallinnossa.

Kuva 8. Tietoturvallisuus sekä normit ja ohjaus.



3 VAHTI -toiminnan organisointi ja kokoonpano

VAHTI kokoontui yhdeksän kertaa vuoden 2015 aikana. VAHTI -johtoryhmään ovat vuoden 2015 aikana kuuluneet:

Puheenjohtaja:

Mikael Kiviniemi	valtiovarainministeriö (1.9.2015 asti)
Aku Hilve	valtiovarainministeriö (2.9.2015 lähtien)

Varapuheenjohtaja:

Esko Vainio	valtiovarainministeriö (1.9.2015 asti)
Sami Kivivasara	valtiovarainministeriö (2.9.2015 lähtien)

Jäsenet, peruskokoonpano:

Tapio Aaltonen	sisäministeriö
Juhani Damski	liikenne- ja viestintäministeriö
Heikki Haukirauma	työ- ja elinkeinoministeriö
Hannu Kuikka	valtioneuvoston kanslia (1.9.2015 asti)
Aino Jalonen	valtioneuvoston kanslia (2.9.2015 lähtien)
Tarmo Maunu	ympäristöministeriö
Harri Mäntylä	puolustusministeriö
Irma Nieminen	opetus- ja kulttuuriministeriö (1.9.2015 asti)
Juho-Antti Jantunen	opetus- ja kulttuuriministeriö (2.9.2015 lähtien)
Tiina Pesonen	sosiaali- ja terveysministeriö
Ari Uusikartano	ulkoasiainministeriö
Antti Vertanen	maa- ja metsätalousministeriö
Anna-Riitta Wallin	oikeusministeriö (1.9.2015 asti)
Matti Aitta	oikeusministeriö (2.9.2015 lähtien)

VAHTIn laajennettuun kokoonpanoon kuuluvat lisäksi:

Reijo Aarnio	Tietosuojavaltuutetun toimisto
Samuli Bergström	Verohallinto
Catharina Candolin	Puolustusvoimat (1.9.2015 asti)
Mano-Mikael Nokelainen	Puolustusvoimat (2.9.2015 lähtien)
Juha Koivisto	Tampereen kaupunki
Tarja Laitiainen	ulkoasiainministeriö, NSA
Heikki Lunnas	Suomen Kuntaliitto
Pentti Mykkänen	Valtiontalouden tarkastusvirasto
Rauli Paananen	Viestintävirasto
Marja Rantala	Maanmittauslaitos
Kimmo Rousku	Valtori (31.5.2015 asti)
Jukka Santala	Väestörekisterikeskus

VAHTI -sihteeristö:

Aku Hilve	valtiovarainministeriö, pääsihteeri (31.5.2015 asti)
Kimmo Rousku	valtiovarainministeriö, pääsihteeri (1.6.2015 lähtien)
Aarne Hummelholm	valtiovarainministeriö
Erja Kinnunen	Valtori
Erka Koivunen	Viestintävirasto (31.7.2015 asti)
Mikko Viitaila	Viestintävirasto (1.8.2015 lähtien)
Minna Romppanen	Maanmittauslaitos (1.8.2015 lähtien)
Esko Vainio	valtiovarainministeriö

Vuonna 2015 VAHTI johtoryhmän kuukausittainen työpanos kokousvalmistelussa ja käsittelyssä on ollut noin 30 htp ja sihteeristön noin 20 htp. Johtoryhmä on kokoontunut yhdeksän kertaa ja sihteeristö yksitoista kertaa toimintavuoden aikana. Tämän lisäksi johtoryhmän, sihteeristön sekä jaostojen jäsenet ovat osallistuneet VAHTI-hankkeiden työhön.

VAHTIn hankkeet on organisoitu siten, että niissä on mukana hankkeen tehtäväalueen edellyttämä hallinnon paras asiantuntemus sekä tarpeen mukaan kuntien ja elinkeinoelämän asiantuntemusta.

4 VAHTIn alajaostot

VAHTIn sihteeristö jatkoi toimintaansa vuonna 2015 ja se on nimetty samaksi toimikaudeksi kuin VAHTI-johtoryhmä. VAHTI tekninen jaosto ja ohjejaosto jatkoivat aktiivista toimintaa. VAHTI perusti kuntien tietoturvajaoston keväällä 2015.

Sihteeristö

Sihteeristön tehtäviä ovat mm.

- valmistella ja dokumentoida johtoryhmän kokoukset
- avustaa toimintasuunnitelmien valmistelussa
- valmistella esitykset toimintakertomuksiksi
- tukea kehittämisohjelmien, hankkeiden ja toimintasuunnitelman koordinointia sekä seurata hankesalkkua
- avustaa hankkeiden perustamisessa ja organisoimisessa
- seurata hankkeiden ja VAHTI-ohjeiston tilannetta ja valmistella siihen liittyviä kehitysehdotuksia
- valmistella toimintaan liittyviä ohjeita, tukimateriaaleja ja muita dokumentteja
- valmistella seminaareja ja muita VAHTI-tapahtumia
- valmistella viestintäsuunnitelma ja toteuttaa viestintäaktiviteetteja
- kehittää sähköisen toiminnan ja turvallisen tiedonvälityksen toimintatapoja
- valmistella tarvittavia VAHTI-esittelymateriaaleja.

VAHTI tekninen jaosto

Teknisen jaoston tehtävänä on

- tulkita kansallisia tietoturvavelvoitteita koskevien tietoturvavaatimuksien ja kriteeristöjen teknisten tietoturvavaatimusten toimeenpanoa.
- tuottaa tulkintojen perusteella teknisen infrastruktuurin, sovellushankkeiden ja hankintojen tueksi esimerkkiratkaisuja ja mahdollisuuksien mukaan yleisimpiä tulkintoja. Kattavien yleistulkintojen teko teknisistä tietojenkäsittely-ympäristöistä ei katsota olevan mahdollista, joten malliratkaisut nähdään tässä toimivana menettelytapana.

- toimia asiantuntijaryhmänä VAHTIssa sekä keskeisissä hankkeissa, joissa roolina on tukea tietoturvavaatimusten ja -kriteeristöjen linjaamista.
- edustaa tieto- ja kyberturvallisuuden näkökulmaa valtionhallinnon keskeisten ICT-hankintojen asiantuntijatukiryhmänä. Ryhmälle tuodaan käsiteltäväksi ja kommentoitavaksi käytettävien tietoturvavaatimusten näkökulmasta kaikki valtionhallinnon keskeiset yhteiset tai hallinnonalojen merkittävät ICT-kilpailutukset.

VAHTI ohjejaosto

Ohjejaoston tehtävänä on

- käydä läpi VAHTIn nykyinen ohjekokonaisuus ja tehdä VAHTIlle esityksiä ohjeiston sisällöstä ja rakenteesta kuten
    - ohjeiden päivittämisestä, yhdistämisestä ja kumoamisesta
    - tarvittavista uusista ohjeista
    - ohjeiden luokittelusta
    - ohjeiston rakenteen kehittämisestä
- valmistella uusien ohjehankkeiden asettaminen
- seurata ja ohjata VAHTIn ohjaamien ohjehankkeiden etenemistä
- käsitellä ohjeet ennen niiden hyväksymiskäsittelyä VAHTI johtoryhmässä
- varmistaa, että ohjeilla on jalkautussuunnitelma ennen VAHTIn hyväksymiskäsittelyä
- edistää ohjekokonaisuutta tukevien sähköisten palvelujen kehittämistä
- toimeenpanna muut VAHTIn ja VAHTIn puheenjohtajan antamat toimeksiannot.

VAHTI kuntien tietoturvajaosto

Kuntajaoston tehtävänä on

- Edistää verkostomaisen toimintatavan kehittämistä kuntien tieto- ja kyberturvallisuusturvatyössä.
- Vauhdittaa ja tehostaa valtionhallinnossa kehitettyjen tieto- ja kyberturvallisuuden hyvien käytäntöjen ja VAHTI-ohjeiden hyödyntämistä ja käyttöä kunnissa.
- Edistää kuntien tietoturvakulttuuria ja osaamisen kehittämistä sekä johdon ja henkilöstön tietoturvatietoisuutta.
- Seurata kuntien tieto- ja kyberturvallisuuden tilannetta hyödyntämällä ja tarvittaessa kehittämällä VAHTIn mittaristoa.
- Analysoida ja tehdä VAHTIlle ja valtiovarainministeriölle esityksiä tieto- ja kyberturvallisuutta koskevan lainsäädännön kehittämisestä kuntien näkökulmista.
- Arvioida ja tarvittaessa valmistella VAHTIlle esitys kuntien tietoturvallisuuden minimitason sääntelystä.

5 Yhteenveto VAHTIn toiminnasta 2015

VAHTI julkaisi vuoden 2015 aikana kaksi uutta julkaisua täydentämään VAHTI-ohjeistoa (ks. liite 2).

VM toteutti ministeriöille ja virastoille kohdistetun valtionhallinnon tietoturvallisuutta koskevan kyselyn, jolla selvitettiin tietoturvallisuuden tilannetta ja kehitystä hallinnossa. Kyselyyn vastasivat kaikki ministeriöt ja suuri osa virastoista. Tulosten yhteenveto on kuvattu luvussa 11.

Keskeisimpiä VAHTI-johtoryhmän käsittelemiä asiakokonaisuuksia ja näkökulmia vuonna 2015 ovat olleet:

- valtionhallintotason tieto- ja kyberturvallisuustyön ja hankkeiden ohjaus
- valtion tietoturvaohjeiden ja -suositusten kokonaisuuden sekä valmistelun ohjaus ja käsittely
- tietoturvallisuuden ja tietoturvakulttuurin vahvistaminen osana hallinnon kaikkea toimintaa
- tieto- ja kyberturvallisuutta koskeva lainsäädännön kehittäminen ja eri normien yhteensovitus
- valtionhallinnon tieto- ja kyberturvallisuuslinjausten käsittely
- tieto- ja kyberturvallisuuden tilanne ja seuranta
- kyberturvallisuusstrategian toimeenpano-ohjelman seuranta
- valtion tietoturvallisuuden periaatepäätöksen ja kehittämisohjelman toimeenpano
- kansainväliset tietoturva- ja tietosuoja-asiat
- korotetun tason tietoturvallisuuden ja ICT-varautumisen yhteishankkeen seuranta
- julkisen hallinnon ICT-hankkeiden ohjelmien ja hankkeiden käsittely
- valtiovarainministeriön SecICT-hankkeen tuottama raportointi.

Sihteeristö on toiminnallaan auttanut hankkeiden seurantaa ja valmistellut VAHTI-johtoryhmän kokouksissa käsiteltyjä asiakokonaisuuksia.

Nykyisen VAHTIn asettamisessa toimikaudelle 1.1.2014–31.12.2016 ja sen toiminnassa on otettu huomioon Suomen kyberturvallisuusstrategia. Asettamispäätöksensä mukaisesti VAHTI tukee valtioneuvostoa ja valtiovarainministeriötä julkisen hallinnon tieto- ja kyber-

turvallisuuteen sekä varautumiseen liittyvässä päätöksenteossa ja valmistelussa. VAHTI on toiminut ja toimii sekä ministeriöiden kyberturvallisuuteen liittyvien strategisten tehtävien että kyberturvallisuusstrategian toimeenpanon koordinaation yhteistyössä muun muassa seuraamalla hallinnonalojen tilannetta kyberturvallisuusstrategian toimeenpanossa.

6 VAHTIn tilaisuudet ja seminaarit

- VAHTI järjesti 12.5.2015 seminaarin tietoturvallisista ICT-hankinnoista.
- VAHTI järjesti 11.11.2015 seminaarin, jossa esiteltiin syksyllä 2015 julkaistun salausohjeen sisältöä ja annettiin ohjeita sen soveltamisesta.
- VAHTI järjesti 13.11.2015 seminaarin Kuntatalolla kuntien keskijohdolle sekä tietohallinto- ja tietoturvavastaaville. Seminaarissa käsiteltiin kuntien tieto- ja kyberturvallisuuden sekä riskienhallinnan tilannetta, haasteita ja kehittämistä.
- Valtionhallinnon vuosittainen tietoturvallisuuden ajankohtaisseminaari valtionhallinnon toimijoille järjestettiin 10.12.2015 valtiovarainministeriössä. VAHTI-päivässä oli noin 150 osallistujaa valtionhallinnon organisaatioista. Tilaisuudessa käsiteltiin mm. tietoturvalainsäädäntöä, häiriötilanteiden hallintaa sekä valtionhallinnon ajankohtaisia tietoturvahankkeita. Valtion johdon puheenvuoron käytti kunta- ja uudistusministeri Anu Vehviläinen.

Ensimmäistä kertaa myönnettävä organisaatiolle tarkoitettu VAHTI-tunnustus myönnettiin Opetushallitukselle. Tunnustuksen perusteluina olivat organisaation jatkuva tietoturvallisuuden kehittäminen sekä osallistuminen VAHTIn asettaman, Valtion tieto- ja viestintätekniikkakeskus Valtorin toteuttamaan korotetun tietoturva- ja varautumisen tason yhteishankkeeseen (KoTVA) ja siinä osoitettu aktiivisuus.

Pitkäaikaisesta, laadukkaasta työskentelystä valtion tietoturvallisuuden kehittämisessä palkittiin VAHTI-viireillä johtava asiantuntija Minna Romppanen Maanmittauslaitoksesta ja sihteeri Aira Vilo valtiovarainministeriön JulkICT-toiminnosta.

VAHTI-hankeryhmät ja jaostot ovat kokoontuneet tavoitteidensa ja hankesuunnitelmiensa mukaisesti.

7 VAHTIn hankkeiden tilanne vuoden 2015 lopussa

Virallisesti asetetut hankkeet löytyvät valtioneuvoston hankerekisteristä. Sieltä näkyvät hankekohtaisesti mm. niiden tehtävät ja niihin osallistuvat henkilöt. Voimassaoleva VAHTI-ohjeisto on esitelty liitteessä 2. Liitteessä 4 on esitetty hankkeet, joissa tehtiin työtä toimintavuoden aikana.

Vuoden 2015 aikana julkaistiin seuraavat VAHTIn julkaisut, suluissa on hankkeen vetäjän nimi

- VAHTIn toimintasuunnitelma vuodelle 2015 (Mikael Kiviniemi, VM/JulkICT)
- VAHTIn toimintakertomus vuodelta 2015, VAHTI 1/2015 (Aku Hilve, VM/JulkICT)
- Ohje salauskäytännöistä, VAHTI 2/2015 (Kimmo Rousku, VM/JulkICT)

Vuoden 2015 aikana käynnistettiin seuraavat uudet hankkeet

- VAHTI kuntien tietoturvajaosto (Harri Ihalainen, Rovaniemen kaupunki)
- VAHTI ohjeistuksen rakenne (Kirsi Janhunen, VM/JulkICT)
- Sähköisen asioinnin tietoturvallisuus (Kimmo Janhunen, Oikeusrekisterikeskus)
- Toiminnan jatkuvuuden hallinta (Riitta Gröhn, Aalto-yliopisto)
- Tietoturvapoikkeamien hallinta (Juha Ilkka, VNK)

Vuoden 2015 aikana on lisäksi tehty työtä seuraavissa VAHTI -hankkeissa

- VAHTIn tekninen jaosto (Kimmo Rousku, Valtori)
- VAHTIn ohjejaosto (Pekka Ristimäki, VRK)
- Korotetun tietoturvatason ja ICT-varautumisen yhteishanke (Hanna Heikkinen, Valtori)
- VAHTI-ohjeiden ruotsiksi kääntäminen (Ralf Sontag, Huoltovarmuuskeskus)
- VAHTI-ohjeiden englanniksi kääntäminen (Tuire Saaripuu, Väestörekisterikeskus)
- Tietoturvallisuuden arvioinnin kehittäminen -hanke (Aku Hilve, VM/JulkICT)

VAHTI toimii seurantaryhmänä seuraavassa valtiovarainministeriön hankkeessa

- Valtion ympärivuorokautisen tietoturvatoiminnan kehittämishanke, SecICT (Kirsi Janhunen, VM)

8 Tieto- ja kyberturvallisuuden tila valtionhallinnossa 2015

VAHTIn vuodesta 2008 lähtien tekemän tietoturvamittarien jatkuvan kehitystyön tuloksena valtion tietoturvallisuuden tilaa voidaan kuvata monipuolisemmin kuin aiemmin. Kyselyä kehitettiin vuoden 2015 osalta ennen kaikkea digitalisoimalla koko kysely käyttäen uutta Valtorin tuottamaa palvelua. Mittariston eräitä kysymyksiä tarkennettiin vuonna 2015, etenkin tietoaineistojen luokitusta ja määrää koskevia kysymyksiä.

Vuosittaisessa seurannassa ei ole pidetty mukana sellaisia tietoturvatoiminnan kehittämisalueita, joissa käytännössä lähes 100 prosenttia virastoista on toteuttanut perustavoitteiden mukaisen toiminnan. Tällainen on esimerkiksi haittaohjelmatorjunta ennen sähköpostien jakelua sekä työasemissa. Vuonna 2015 päästiin 100 prosenttiin kaikkiaan neljässä mittarissa:

- Tietoturvavastaava (osa/ kokopäiväinen),
- Vakavista tietoturvapoikkeamista johdolle raportointi
- Huonotasoisten salasanojen käytön esto
- Tietoturvapoikkeamien käsittely on organisoitu / vastuutettu.

VAHTIn seuranta osoittaa, että kokonaisuutena valtion tieto- ja kyberturvallisuuden tilanne pysyi lähes samalla tasolla kuin edellisenä vuonna. Tämä on seurausta osittain vuosien 2010–2015 aikana tehdystä aktiivisesta, tietoturvallisuusasetuksen edellyttämästä kehitystyöstä, joka on asteittain tasoittunut vuoden 2015 aikana. Osittain tuloksiin vaikuttavat:

- lukuisat valtionhallinnon rakenteisiin liittyvät muutokset, esimerkiksi Valtorin toiminnan asteittainen käynnistyminen, VNHY:n toiminnan käynnistyminen
- taloudellinen tilanne.

Toisaalta seuranta osoittaa, että VAHTIn tietoturvatyössä aktiivisesti mukana olleiden organisaatioiden tilanne on edelleen selvästi parempi kuin yhteistyössä vähän tai ei ollenkaan mukana olleiden. Tähän vaikuttaa myös organisaation asettamat omat vaatimukset ja vaatimustaso; esimerkiksi turvaviranomaisten asettama turvallisuuden taso on korkeampi keskimäärin, mikä näkyy myös VAHTI-tuloksissa heidän osaltaan parempina tuloksina.

VAHTI kiinnittää huomiota siihen, että raportoitavat tulokset ovat ministeriöiden, virastojen ja laitosten omia arvioita suhteessa käytettyihin mittareihin. Jokainen vastaajaorganisaatio saa palautetiedon kyseisen organisaation tilanteesta verrattuna koko valtionhallinnon sekä oman hallinnonalan keskiarvotietoihin.

Tieto- ja kyberturvallisuuden hallinta ja johtaminen sekä tietotekninen turvallisuus 2015

Aiempiin vuosiin verrattuna osassa kehittämiskohteista on vuonna 2015 edelleen saatu aikaan parannuksia. Kaikkiaan 21 kysymyksen tulokset on pysynyt samana tai parantunut ja samoin 21 kysymyksen tulokset ovat laskeneet. Vuoteen 2014 verrattuna suurimmat parannukset on saatu aikaan seuraavissa kohteissa:

Mittari	v. 2015	v. 2014
• Toipumissuunnitelma	71 %	57 %
• Johdon sisäisen valvonnan ja riskienhallinnan arviointi- ja vahvistuslausumassa käsitellään tietoturvariskejä	81 %	70 %
• Keskeisten tietojärjestelmien tietoturva-arviointi	86 %	77 %
• Ydintoimintojen riskien arviointi ja dokumentointi	76 %	67 %
• Valmiussuunnitelma	78 %	72 %

Erityisesti kehittyneitä ovat toiminnan häiriöiden varautumiseen liittyvät osa-alueet, joka mikä näkyy sekä toipumis- että valmiussuunnitelmien määrän kasvuna.

Edelliseen vuoteen verrattuna kielteisin kehitys on tapahtunut seuraavissa kohteissa:

Mittari	v. 2015	v. 2014
• Rekisteriselosteet verkkosivuilla	54 %	65 %
• Tietoturvallisuus arvioitu VAHTI-ohjeisiin / standardeihin peilaten	82 %	92 %
• IDS käytössä	59 %	69 %
• Säännöllinen johdolle raportointi tietoturvallisuudesta	90 %	98 %
• Haittaohjelmatarkistus HTML-sivuille	88 %	97 %
• Tunnistettu sidosryhmät, joille organisaatiolla on tietoturvavastuita	78 %	87 %
• Tietoturvatavoitteet tulosohjauksessa	71 %	80 %

Selvästi heikoin tulos saatiin edelleenkin jatkuvuussuunnitelmien harjoittelussa, vaikka tulos olikin edellistä vuotta parempi eli noussut 18 prosentista 22 prosenttiin, mikä tarkoittaa neljän prosentin parannusta.

VAHTI-ohjeisiin perustuva tietoturvallisuuden arviointien väheneminen on seurausta siitä, että tietoturvallisuusasetuksen kolmen vuoden siirtymäkausi päättyi vuonna 2013. Tämän johdosta laajamittainen tarve tehdä näitä arviointeja on vähentynyt aiemmista vuosista.

Kuvan 9 taulukossa esitetään valtion tietoturvallisuuden tilannetta vuonna 2015 VAHTIn tietoturvamittarien avulla. Tässä taulukossa eivät ole mukana kyberturvallisuuden eivätkä tietoturvallisuuden perustason ja luokituksen mittarit, joita kuvataan omissa luvuissaan.

Kuva 9. Tietoturvallisuuden hallinta ja johtaminen valtionhallinnossa 2011 - 2015 – osa 1.

Tietoturvallisuuden hallinta ja johtaminen	2015	2014	2013	2012	2011
	prosentteja organisaatioista				
Tietoturvavastaava (osa / kokopäiväinen)	100	100	100	93	90
Vakavista tietoturvapoikkeamista johdolle raportointi	100	100	100	100	96
Huonotasoisten salasanojen käytön esto	100	98	93	97	92
Tietoturvapoikkeamien käsittely organisoitu / vastuutettu	100	97	99	92	87
Tietoturvapolitiikka	98	98	87	90	82
Sovittu käyttövaltuuksien hallintaperiaatteet	98	97	95	97	92
Varmuuskopioiden suunnitelmallinen hallinta	98	97	89	100	96
Tunnukset / valtuudet käyttövaltuushallintaperiaatteiden mukaisesti	98	95	95	95	91
Tekninen valvonta käsitelty YT-menettelyssä	95	100	89	87	78
Vakavista tietoturvapoikkeamista pidetään kirjaa	95	98	88	85	82
Johdon hyväksymät sähköpostien pelisäännöt	95	95	90	73	82
Tietojen suojausluokkien mukainen tilojen eriyttäminen	93	88	73	83	73
Keskeiset osa-alueet kattava tietoturvaohjeisto	92	92	93	92	85
Viestinvälityksen ja sähköpostien salaus käytössä	92	90	92	78	78
Salaus tiedostoissa, hakemistoissa ja kovalevyissä	92	88	87	87	82
Erilliset tietojenkäsittelyn toimintaympäristöt	92	95	83	92	82
Säännöllinen johdolle raportointi tietoturvallisuudesta	90	98	83	85	63
Eri toiminnot kattava tietoturvayhteistyöryhmä	90	92	81	85	76
Haittaohjelmatarkistus HTML-sivuille	88	97	83	82	78
Keskeisten tietojärjestelmien tietoturva-arviointi	86	77	64	70	57
Toimintaverkostojen ja alihankkijoiden hallinta	85	90	86	87	86

Kuva 9. Tietoturvallisuuden hallinta ja johtaminen valtionhallinnossa 2011 - 2015 – osa 2.

Tietoturvallisuuden hallinta ja johtaminen	2015	2014	2013	2012	2011
	prosentteja organisaatioista				
Eriytetty tietoverkon eri suojaustasoa vaativat osat (+ rajoitus)	83	87	80	90	86
Palvelutoimittajien turvallisuusselvitykset	83	82	73	75	75
Tietoturvallisuus arvioitu VAHTI-ohjeisiin / standardeihin peilaten	82	92	78	90	76
Säännöllinen tietoturvariskien arviointi	81	85	77	72	57
Prosessien ja riippuvuuksien tunnistaminen	81	82	73	80	80
Johdon sisäisen valvonnan ja riskienhallinnan arviointi- ja vahvistuslausumassa käsitellään tietoturvariskejä	81	70	54	67	49
Tunnistettu sidosryhmät, joille organisaatiolla on tietoturva-vastuita	78	87	75	75	63
Valmiussuunnitelma	78	72	69	67	69
Ydintoimintojen riskien arviointi ja dokumentointi	76	67	54	53	53
Turvallisuusselvitysmenettely käytössä	73	77	70	73	65
Tietoturvasuunnitelma	73	67	81	75	67
Tietoturvatavoitteet tulosohjauksessa	71	80	72	65	53
Toipumissuunnitelma	71	57	57	42	46
Riskienhallintapolitiikka	68	72	49	50	46
Ydinprosesseissa tietoturvatavoitteet	66	68	58	45	55
Jatkuvuussuunnitelma	63	65	58	40	40
Järjestelmämääritysten tietoturvavaatimusten auditointi	61	63	53	58	54
Valtorin IHRS-palvelu käytössä	61				
IDS käytössä	59	69	55	63	48
Rekisteriselosteet verkkosivuilla	54	65	59	60	63
Kokopäivätoiminen tietoturvavastaava	42	45	31	35	35
Jatkuvuussuunnitelma harjoiteltu	22	18	11	23	15

Haittaohjelmilta ja tietoturvahyökkäyksiltä suojautuminen sekä muu tietotekninen turvallisuuden kehittäminen on ollut keskeinen osa jatkuvaa valtion organisaatiossa toteutettavaa tietoturvatyötä. Tietoteknisen tietoturvallisuuden kehittymisen esimerkkejä ovat:

- Kaikissa vastaajaorganisaatioissa on käytössä huonotasoisten salasanojen käytön esto
- Varmuuskopioiden suunnitelmallinen hallinta on hoidettu hyvin 98 prosentissa vastaajaorganisaatioissa
- Käyttövaltuuksien hallinta on hoidettu hyvin 98 prosentissa organisaatioita. VAHTI ohjeisti käyttövaltuushallintaa jo vuonna 2006
- Viestinvälityksen ja sähköpostien salaus on käytössä 92 prosentilla organisaatioista.

Vaikka vuonna 2015 tilannetta saatiin merkittävästi parannettua, kokopäivätoimisia tietoturvavastaavia on koko valtionhallinnon tasolla (42 prosenttia vastaajista), laskua edelliseen vuoteen 3 prosenttia. Tässä esimerkiksi Valtoriin ja mahdollisesti Valtioneuvoston kansliaan tehdyt toimintasiirrot ovat vaikuttaneet tulokseen.

Useimmissa organisaatioissa tulisi edelleen jatkaa valmius-, tietoturva- ja jatkuvuussuunnittelun kehittämistä ja toteuttamista sekä erityisesti huolehtia rekisteriselosteiden ajantasaisuudesta ja saatavuudesta.

Jatkossa entistä tärkeämpi kehitettävä ja ylläpidettävä asia koskee riskien ja jatkuvuudenhallinnan sekä varautumisen toteuttamista ja kehittämistä. Seuraavien vuosien aikana digitalisoidaan lukuisia valtion- ja julkishallinnon prosesseja sekä palveluita. Tässä muutoksessa pitää pystyä ennakoimaan siitä aiheutuvat uhat ja ottamaan tunnistetut riskit paremmin seurantaan ja hallintaan.

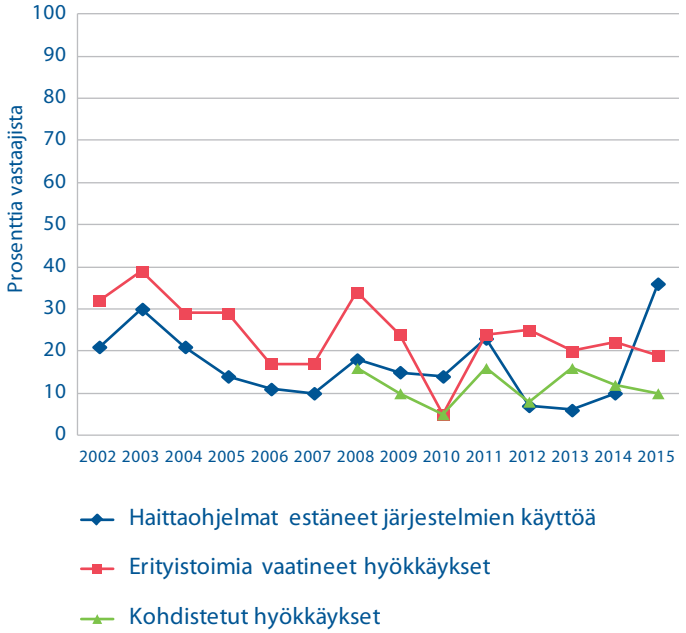
Jatkuvuudenhallinta ja varautuminen nousevat myös normaalioloissa keskeiseen rooliin toiminnassa tulee ennakoidusti varautua erilaisilla keinoilla toiminnan jatkuvuuden takaamiseen ja varautumisen avulla huolehtia tarvittavista prosesseista häiriötilanteiden hallinnan osalta. Häiriötilanne voi syntyä hyvin erilaisista syistä; inhimillinen erehdys, luonnonilmiö, tekninen vika, tietoturvapoikkeama tai toteutunut kyberuhka.

Seurannassa kerätty tieto osoittaa selvästi, että annettu valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä keskittyy juuri niiden asioiden parantamiseen, joissa valtionhallinnossa on merkittävää kehittämistarvetta; johtaminen, kokonaisvaltaisuus ja läpäisy, ennaltaehkäisy ja varautuminen sekä tiedon ja sen arvon suojaaminen.

Tietoturvaongelmat

Kuvasta 10 näkyy haittaohjelmista aiheutuneen järjestelmien käytön estymisen ja erityistoimia vaatineiden tietoturvahyökkäysten yleisyyden kehitys vuosina 2002–2015. Järjestelmät tai niiden osa on ollut haittaohjelmien takia pois käytöstä noin 36 prosentilla organisaatioista vuonna 2015. Tässä on merkittävä nousu (26 prosenttiyksikön kasvu) edelliseen vuoteen verrattuna. Tulos vastaa hyvin Kyberturvallisuuskeskuksen havaintoja ja varoituksia Suomessa levinneistä haittaohjelmista vuonna 2015. Haittaohjelmien aiheuttamat haitat valtionhallinnossa ovat siis nousseet edelliseen vuoteen verrattuna. Järjestelmäkatkoja ei ole luokiteltu niiden keston tai laajuuden perusteella.

Kuva 10. Tietoturvaongelmien yleisyys valtionhallinnossa.



Erityistoimia aiheuttaneita ulkopuolisia hyökkäyksiä on havainnut noin 19 prosenttia, ja noin 10 prosenttia valtionhallinnon organisaatioista on havainnut joutuneensa kohdistetun hyökkäyksen kohteeksi vuonna 2015. Erityistoimia vaatineiden hyökkäyshavaintoja tehneiden organisaatioiden prosenttiosuus on hieman laskenut (22 prosentista 19 prosenttiin) samoin kun kohdistettujen hyökkäysten havainnointimäärä on laskenut (kaksi prosenttia, 12 prosentista 10 prosenttiin). Organisaatioiden hyökkäysten havainnointikeinojen määrä on hiukan parantunut.

VAHTI kiinnittää huomiota siihen, että kansainvälisten selvitysten mukaan piiloon jäävien hyökkäysten osuuden arvioidaan olevan kasvussa ja havainnointikyvyn kehittämisen tulee olla yksi keskeisimpiä teknisen tietoturvallisuuden kehitysalueita seuraavien vuosien aikana.

Keinoja, joita valtionhallinnon organisaatiot käyttävät tietoturvahyökkäysten havaitsemiseksi ovat mm. erilaiset **tekniset ratkaisut,** kuten skannaukset, IDS/IPS, IRHS, HAVARO, palomuurin ja palvelinten lokiseuranta sekä virustorjunta. Toiminnallisista ja hallinnollisista keinoista voidaan mainita **oman henkilöstön** ilmoitukset, **palveluntarjoajan** ilmoitukset sekä erilaiset kansalliset ja kansainväliset **yhteistoimintaverkostot**. Organisaatioilla on tyypillisesti käytössään useita keinoja tästä valikoimasta. Pääosin vuonna 2015 on toteutettu samoja teknisiä keinoja kuin aikaisemmin, keskitettyjen lokienhallintajärjestelmien käyttö on jonkin verran yleistynyt.

Erilaisista havaituista tietoturvapoikkeamatyypeistä olivat vastausten perusteella yleisempiä järjestelmien tai työasemien toimintaan vaikuttaneet **haittaohjelmat**. Näistä ei kui-

tenkaan ole ilmoitettu aiheutuneen esimerkiksi merkittäviä, laajavaikutteisia toiminnan keskeytyksiä. Toiseksi laajimman poikkeamatyypin muodostavat **palvelunestohyökkäykset, sen jälkeen huijausviestit ja haavoittuvuudet**. Tietoturvapoikkeamiin varautumista ja niiden riskin vähentämistä vaikeuttaa se, että seurannan perusteella erilaisia toteutuneiden poikkeamien tyyppejä on entistä enemmän. Ennakoiva laaja-alainen tietoturvatyö pienentää riskejä. Tietoturvapoikkeamien varalle pitää olla hyvät etukäteisvalmistelut eli oma prosessi, jonka mukaan häiriötilanteiden hallinta toteutetaan. Häiriötilanteiden hallintaa kehitetään myös osana VM:n toteuttamaa SecICT-hankkeen VIRT-toimintaa (Virtual Incident Response Team).

Kuva 11. Sanapilvi vastaajien tietoturvapoikkeamista vuonna 2015. Aikaisempiin vuosiin verrattuna kyselyssä ilmeni yhä enemmän erilaisia tietoturvapoikkeamien tyyppejä, erityisesti ilmoitettujen palvelunestohyökkäysten määrä on noussut.

Raportoidut tietoturvallisuuteen käytetyt resurssit ja tapahtumamäärät

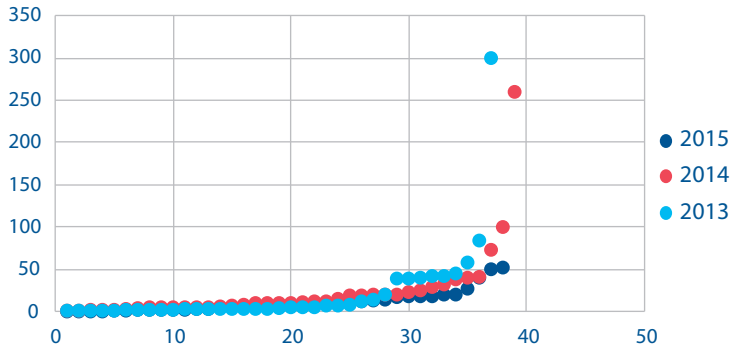
Osana VAHTIn seurantaa ja mittaristoa seurattiin nyt kuudetta kertaa tietoturvallisuuteen käytettyjä vastanneiden organisaatioiden henkilö- ja talousresursseja ja tapahtumamääriä. Osassa toimijoita seurannan kohteena olevia asioita ei järjestelmällisesti seurata. Yhteenvetona VAHTIlle raportoiduista resursseista ja määristä voidaan todeta:

- **Haavoittuvuuksien korjaamiseen** raportoitiin käytetyn keskimäärin 21 henkilötyöpäivää vuonna 2015 näitä seuranneissa 50 organisaatiossa (2014: 19 henkilötyöpäivää). **Haavoittuvuuksien korjaamiseen organisaatiot ilmoittivat käyttäneensä keskimäärin 6 200 euroa (2014: 47 00 €).** Yhdeksässä organisaatioissa ei seurata erikseen haavoittuvuuksien korjaamisen henkilötyöpanostuksia tai taloudellisia kustannuksia.
- **Tietoturva-arviointeihin** raportoitiin käytetyn keskimäärin **22 000 euroa** / organisaatio (2014: 20 200 euroa) ja **keskimäärin 22** oman henkilökunnan henkilötyöpäivää (2013: 28). Raportoidut taloudelliset investoinnit ovat nousseet jonkin verran edellisestä vuodesta, vastaavasti oman työmäärän osuus on pienentynyt.

- **Tietoturva- ja kyberongelmien** välittömiä kustannuksia raportoitiin VAHTIlle **keskimäärin 14 500 euron** edestä (2014: 38 200 euroa). Tämä tarkoittaa sitä, että tieto- ja kyberturvaongelmien välittömät kustannukset vähenivät 38 prosenttia.

Organisaatioiden riskienhallintaraportointiin kirjattiin keskimäärin 11 tietoturvapoikkeamaa (2014: 23,5 poikkeamaa). Kuvassa 12 näkyy, että poikkeamia raportoineissa organisaatiossa suuret havaintomäärät keskittyvät pienelle määrälle toimijoita. Tämä selittyy niin organisaatioiden koolla, raportointikäytännöillä, kuin myös toimialoilla, joilla eniten poikkeamia raportoineet toimivat. Tietoturvapoikkeamien käsittelykulttuuri näyttää vahvistuvan osassa organisaatioita, mutta monilla tällainen toimintatapa ei ole vielä vakiintunut tai alkanut osana riskienhallintaa.

Kuva 12. Organisaatioiden riskienhallinnassa raportoituja tietoturvapoikkeamia. Nollasta poikkeavat määrät esitettynä organisaatioittain vuosilta 2013–2015. Erityisesti vuoden 2015 osalta tulee huomata, että suurin yksittäinen vastaus oli 52 poikkeamaa, kun vuonna 2014 kahdella organisaatiolla havaittiin yli 250 tietoturvapoikkeamaa.



Kyselyssä seurattiin monesta eri näkökulmasta tietoturvallisuuteen käytettyjä keskimääräisiä resursseja ja lukumääriä vastanneissa organisaatioissa. Kuvan 13 taulukossa on yhteenvetoa keskimääräisistä tiedoista vastanneissa organisaatioissa. Osassa toimijoita seurannan kohteena olevia asioita ei mitata eikä seurata organisaation tasolla lainkaan. Vastaajien kokonaislukumäärä on laskenut ainakin sen vuoksi, että useammat hallinnonalat ovat siirtyneet antamaan kokonaisvastauksia keskusvirastojen kautta, tai osana Valtorin tuottamaa raportointia. Tämä vaikuttaa niihin tunnuslukuihin, joissa lasketaan keskiarvoja.

Yhteenvetoa keskimääräisistä resursseista ja volyymeista vuosina 2010–2015 esitetään seuraavassa taulukossa. Tässä otetaan huomioon vain ne toimijat, jotka ovat mitanneet asiaa ja joiden vastaus poikkeaa nollasta.

Kuva 13. Tietoturvallisuuteen käytettyjä resursseja ja volyymeja

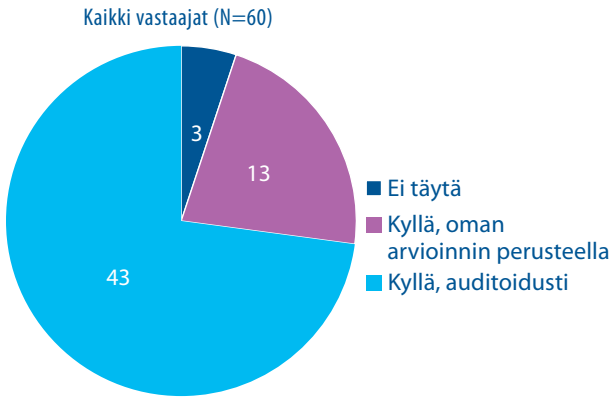
Seurannan kohda	Toteutuneet keskiarvot (nollasta poikkeavat)					
	2015	2014	2013	2012	2011	2010
Tieto- ja kyberturvaongelmien aiheuttamat suorat kustannukset euroa / organisaatio	14 500	38 200	78 400	15 500	16 900	9 600
Raportoitujen tietoturvapoikkeamien lukumäärä kpl / organisaatio	11	23,5	74	16	6	25
Tietoturvahaavoittuvuuksien korjaamisen oma työ htp / organisaatio	21	19	44	56	51	32
Tietoturvahaavoittuvuuksien korjaamisen suorat kustannukset euroa / organisaatio	6 200	4 700	47 900	29 700	15 400	66 700
Tietoturvakoulutukseen osallistuminen oma työaika htp / organisaatio	-	133	80	178	33	61
Tietoturvakoulutukseen käytetyt ostopalvelut euroa / organisaatio	-	10 800	11 700	22 400	26 300	16 500
Tietoturva-arviointeihin käytetty oma työaika htp / organisaatio	22	28	28	137	24	43
Tietoturva-arviointeihin käytetyt ostopalvelut euroa / organisaatio	22 000	20 200	26 700	41 100	27 300	40 500

Tietoturvallisuusasetuksen täytäntöönpanon tilanne

VAHTI selvitti 1.10.2010 voimaan tulleen tietoturvallisuusasetuksen täytäntöönpanon tilannetta ministeriöissä ja virastoissa vuoden 2015 lopussa. Kuvassa 15 esitetään organisaatioiden omien arvioiden jakauma sen suhteen, mikä on organisaation tilanne tietoturvallisuusasetuksen 5 §:n vaatimusten eli tietoturvallisuuden perustason toteuttamisessa.

Vastausten perusteella 73 prosenttia (2014: 68 prosenttia) virastoista täyttää tietoturvallisuuden perustason vaatimukset auditoinnin perusteella ja lisäksi 22 prosenttia (2014: 15 prosenttia) ilmoitti täyttävänsä perustason vaatimukset itsearvioinnin perusteella. Viisi prosenttia ei täytä perustasoa, parannusta tässä on kuitenkin 12 prosenttiyksikköä vuoteen 2014 verrattuna (2014: 83 prosenttia).

Kuva 14. Tietoturvallisuusasetuksen 5 §:n vaatimusten toteutus. 95 prosenttia vastaajista täyttää vaatimukset vuoden 2015 lopussa.



Virastojen omat arviot tilanteestaan VAHTI 2/2010 -ohjeessa linjattujen tietoturvatasojen toimeenpanossa selvitettiin vuoden 2015 lopussa. Selvitys kohdistettiin erityisesti tietoturvallisuuden hallintaan, johtamiseen ja tietojärjestelmien hallintaan.

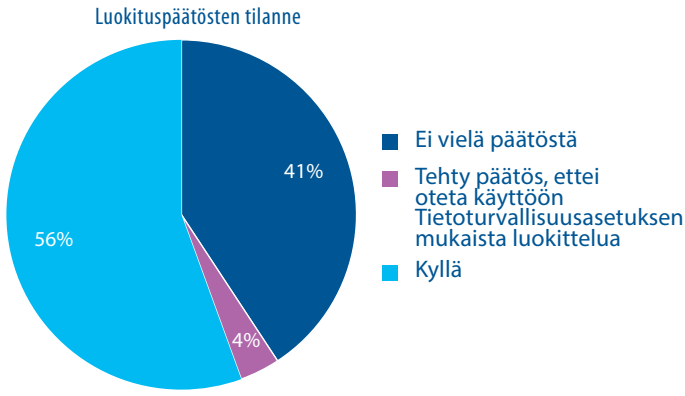
Tulokset on kuvattu kuvassa 15, jossa esitetään kultakin osa-alueelta prosenttijakautuma virastoista. Vuoden aikana kaikissa osa-alueissa on tapahtunut pientä kehitystä siten, että osa organisaatioista on saavuttanut oman arvionsa mukaisesti korotetun tai korkean tason kaikissa kolmessa osa-alueessa.

Kuva 15. Virastojen arvioiman tietoturvallisuuden tason jakauma niiden omassa toiminnassa vuonna 2015 (suluissa vuoden 2014 jakauma).

Viraston arvioima tietoturvataso	Tietoturvallisuuden hallinta	Tietoturvallisuuden johtaminen	Tietojärjestelmien hallinta
korkea tai korotettu	2 (0) %	7 (3) %	2 (2) %
perustaso	88 (83) %	85 (87) %	90 (85) %
perustaso ei täyty	10 (17) %	8 (10) %	8 (13) %

Tämän lisäksi selvitettiin tilanne tietoaineistojen luokituksessa sekä organisaatiossa käsiteltävissä salassa pidettävissä tietoaineistoissa, ja käsittelyn jakauma suojaustasoittain. Asian selvittäminen oli tärkeää 1.10.2010 voimaan tulleen tietoturvallisuusasetuksen toimeenpanon ohjaamisen ja seuraamisen kannalta sekä kansallisen ja kansainvälisen suojausluokitellun materiaalin rinnastettavuuden osalta. Luokituspäätökset edistävät suojattavan aineiston välittämistä organisaatioiden välillä.

Kuva 16. Luokituspäätösten tilanne vuoden 2015 lopussa. Vastanneista organisaatioista 56 prosenttia ilmoitti tehneensä päätöksen tietoaineistojen luokituksesta vuonna 2015 tai aikaisemmin. Vuonna 2014 58 prosenttia oli tehnyt päätöksen, nyt laskua kaksi prosenttiyksikköä, syynä hieman eri vastaajat. Vastaavasti ”Ei vielä päätöstä”-osuus on noussut 37 prosentista neljällä prosentilla 41 prosenttiin. Päätös, ettei oteta käyttöön luokittelua, on osuudeltaan vastaavasti laskenut viidellä prosenttiyksiköllä alaspäin neljään prosenttiin vuonna 2015.



Kuvassa 17 kerrotaan virastojen vastauksiin perustuvat jakautumat korkeimmista organisaatioissa käsiteltävistä kansallisten ja kansainvälisten tietoaineistojen suojaustasoista.

Kuva 17. Tietoaineistojen korkein suojaustaso

Korkein organisaatiossa käsiteltävien salassa pidettävien tietoaineistojen suojaustaso	Kansalliset tietoaineistot	Kansainväliset tietoaineistot
Suojaustaso I	14 (18) %	7 (5) %
Suojaustaso II	44 (37) %	4 (17) %
Suojaustaso III	39 (40) %	16 (22) %
Suojaustaso IV	4 (5) %	16 (10) %
ei käsitellä lainkaan	-	58 (46) %

Kansallisia ST IV -tietoaineistoja käsittelee ainoastaan neljä prosenttia vastaajista eli käytännössä kaksi organisaatiota. Vastaavasti ST II -tason tietoaineistoja käsittelee seitsemän prosenttia useampi kuin v. 2014 eli 44 prosenttia.

Vastaajista 58 prosenttia (v. 2014: 46 prosenttia) ilmoitti, ettei käsittele ollenkaan kansainvälisten tietoturvavelvoitteiden piirissä olevia salassa pidettäviä tietoaineistoja. ST IV- ja III -tietoaineistoja käsittelee korkeimpana tasona molempia 16 prosenttia vastaajista.

VAHTI pitää tärkeänä, että panostuksia luokituspäätösten ja luokitusten mukaisten vaatimusten toteuttamisessa jatketaan. Valtioneuvoston kansliaan perustetulla Valtioneuvoston hallintoyksiköllä on tärkeä rooli asian edistämisessä valtioneuvostossa ja sen toiminnoissa ja ratkaisuissa.

Kyberturvallisuusstrategian täytäntöönpanon tilanne

VAHTI ja Turvallisuuskomitea ovat Suomen kyberturvallisuusstrategiassa korostetut toimielimet. VAHTIssa seurataan säännöllisesti kyberturvallisuusstrategian toimeenpanoa hallinnonaloilla. Seurannan tehostamiseksi VM valmisteli raportoinnin mallipohjan ja esitteli VM:n vastuulla olevien toimenpiteiden tilannetta. VM:llä on ministeriöistä vastuullaan eniten toimenpiteitä. VAHTIssa käsiteltiin Turvallisuuskomitean ja Kyberturvallisuuskeskuksen tilannekatsauksia.

VAHTI valmisteli yhteistyössä Turvallisuuskomitean kanssa kyberturvallisuuden seurannan kysymyssarjan osaksi VAHTIn kyselyä ensimmäisen kerran osaksi vuoden 2014 kyselyä, ja nyt samat kysymykset on kysytty toistamiseen.

VAHTIn kyselyssä kyberturvallisuuden selvitys hoidettiin kahdeksalla kypsyystasomittarilla. Jakaumat ovat seuraavat:

1. Toimintayksiköiden ja organisaation tietohallinnon (tai vastaavan) välinen yhteistyö häiriötilanteessa

Toimintayksikön ja organisaation tietohallinnon (tai vastaavan) välistä yhteistoimintaa ei ole suunniteltu toimintayksikön toimintaa haittaavien vakavien tietoteknisten häiriöiden varalle. Kun tietotekninen häiriö havaitaan, käynnistyy organisaation tietohallinnon (tai vastaavan) toimesta selvitys häiriön luonteesta. Tiedostetaan tietoteknisen häiriön vaikuttavan liiketoimintaan (sisäiset ja ulkoiset asiakkaat). Saattaa olla tiedostettu tarve täsmentää organisaation tietohallinnon (tai vastaavan) toiminnan jatkuvuuden turvaavat tietotekniset tehtävät, menettelyt ja tekniset ratkaisut.	31 %
Vakavassa tietoteknisessä häiriötilanteessa toimitaan toimintayksikön ja organisaation tietohallinnon (tai vastaavan) kesken sovitun toimintatavan mukaisesti. Toimintayksikön ja organisaation tietohallinnon (tai vastaavan) kesken on tunnistettu vakavassa häiriötilanteessa suorittamatta jäävien liiketoimintatehtävien merkitys liiketoiminnalle (sisäisille tai ulkoisille asiakkaille) ja arvioitu häiriön aiheuttamat kustannukset.	36 %
Vakavassa tietoteknisessä häiriötilanteessa toimintayksikön ja organisaation tietohallinnon (tai vastaavan) jatkuvuussuunnitelmat ohjaavat yhteistoimintaa. Suunnitelmat sisältävät toiminnan ohjaamisen ja vahinkojen rajoittamisen toimenpiteet, toteutettavat toimintayksikön liiketoimintatehtävät (ml. välineet) ja organisaation tietohallinnon (tai vastaavan) tehtävät sekä tarvittavien muiden toimintayksiköiden, tukitoimintayksiköiden ja ulkoisten toimijoiden tehtävät (ml. välineet). Tehtävät ovat vastuutettu. Tilanteen selvittämiseksi on riittävästi päteviä henkilöitä. Vastaava häiriö pyritään jatkossa ehkäisemään.	29 %
Vakavassa tietoteknisessä häiriötilanteessa toimintayksikön ja organisaation tietohallinnon (tai vastaavan) yhteistoiminnan jatkuvuus varmistetaan jatkuvuussuunnitelmiin dokumentoiduilla ja käyttöönotetuilla toimenpiteillä. Keskinäinen yhteistoiminta ja muu yhteistoiminta tarpeellisten toimintayksiköiden, tukitoimintayksiköiden ja ulkoisten toimijoiden kanssa on selvästi määritelty. Toimintayksikkö ja organisaation tietohallinnon (tai vastaavan) ovat tietoisia toistensa tehtävistä ja jatkuvuudenhallinnan menettelyistä. Häiriön aikaansaanut syy pyritään poistamaan välittömästi.	5 %
Vakavassa häiriötilanteessa toimintayksikön ja organisaation tietohallinnon (tai vastaavan) yhteistoiminnan jatkuvuus kyetään varmistamaan säännöllisesti arvioiduilla ja harjoitelluilla toimintayksikön ja organisaation tietohallinnon (tai vastaavan) sekä muiden tarvittavien ulkoisten toimijoiden jatkuvuudenhallinnan menettelyillä liiketoimintavaikutukset (ulkoiset ja sisäiset asiakkaat) minimoiden.	0 %

2. Tietoresurssien kriittisyys ja korvattavuus

Tietoresursseihin (mm. tietoaineistot, tietokannat, tiedostot, asiakirjat, sovellukset, järjestelmät, tietokoneet, tietoverkot) liittyviin häiriöihin (mm. saanti- ja käyttöhäiriöt, laiterikot, tietoliikennehäiriöt) reagoidaan niiden tapahduttua. Saattaa olla, että on tiedostettu liiketoiminnan riippuvuus sisäisistä tietoresursseista ja tarve arvioida sisäisten tietoresurssien kriittisyydet.	27 %
Tietoresurssit (mm. tietoaineistot, tietokannat, tiedostot, asiakirjat, sovellukset, järjestelmät, tietokoneet, tietoverkot) on tunnistettu ja kriittisyysluokiteltu. On tiedostettu tarve varmistaa kriittisille tietoresursseille häiriötilanteissa tarvittavat korvaavat tai vaihtoehtoiset tietoresurssit.	46 %
Toiminnan suunnittelua ja tietoresurssien käytön mitoittamista ohjaa periaate, että häiriö yksittäisen resurssin saatavuudessa ei saa vaikuttaa toimintaan. On kartoitettu kriittisille tietoresursseille häiriötilanteissa tarvittavia korvaavia / vaihtoehtoisia resursseja ja niiden toimittajia. Korvaavat / vaihtoehtoiset resurssit on otettavissa käyttöön lyhyellä viiveellä.	22 %
Tietoresurssien kriittisyysluokittelu tarkistetaan säännöllisesti. Kriittisille tietoresursseille on korvaavat / vaihtoehtoiset resurssit, jotka ovat tarvittaessa heti käyttöönotettavissa. Tarvittavien toimittajien kanssa on tehty sopimukset korvaavien / vaihtoehtoisten tietoresurssien toimittamisesta.	5 %
Arvioinnit osoittavat, että säännöllinen tietoresurssien kriittisyysluokittelu ja korvaavien resurssien käyttömahdollisuus tukevat jatkuvuudenhallinnan kehittämistä ja täten vähentävät häiriöistä aiheutuvia kustannuksia.	0 %

3. ICT-varautuminen

ICT-varautumisen ja jatkuvuudenhallinnan (mm. harjoitusten, ohjeiden, toimintatapojen, järjestelyjen tai teknisten ratkaisujen) kehittämishankkeista ei ole näyttöä tai hankkeet ovat puhetasolla.	3 %
ICT-varautumisen ja jatkuvuudenhallinnan (mm. harjoitusten, ohjeiden, toimintatapojen, järjestelyjen tai teknisten ratkaisujen) kehittämishankkeista on jonkin verran näyttöä. On esimerkiksi tunnistettu tietotekniikkaan ja / tai automaatiojärjestelmiin liittyviä riskejä.	36 %
ICT-varautumisen ja jatkuvuudenhallinnan (mm. harjoitusten, ohjeiden, toimintatapojen, järjestelyjen tai teknisten ratkaisujen) kehittämishankkeista on näyttöä. Toiminta on ohjeistettu tai on suunniteltu vaihtoehtoiset toimintatavat häiriötilanteen varalle.	46 %
Tietoteknisen toimintavarmuuden ja jatkuvuudenhallinnan kehittämishankkeista on selvää näyttöä. Toimintatapoja, järjestelyjä ja teknisiä ratkaisuja kehitetään systemaattisesti. Esimerkiksi arviointien perusteella on kehitetty tietoteknisten kumppaneiden kanssa sopimuksissa sovittuja jatkuvuudenhallinnan menettelyjä.	14 %
ICT-varautumisen ja jatkuvuudenhallinnan kehittämishankkeista on laaja-alaista näyttöä. Harjoituksia, ohjeita, toimintatapoja, järjestelyjä ja teknisiä ratkaisuja kehitetään systemaattisesti. Esimerkiksi harjoitusten avulla on kehitetty tietoteknisten kumppaneiden kanssa sopimuksissa sovittuja jatkuvuudenhallinnan menettelyjä.	2 %

4. Kyber- ja tietoturvariskien hallintaprosessi (tunnistus, arviointi, toimenpiteet)

Kyber- ja tietoturvariskien hallintaprosessia (tunnistus, arviointi, toimenpiteet) ei ole.	2 %
Kyber- ja tietoturvariskienhallintaprosessi (tunnistus, arviointi, toimenpiteet) aloitetaan tapauskohtaisesti. Organisaation tietohallinto (tai vastaava) tunnistaa itsenäisesti järjestelmien ja tietoverkkojen uhkia ja haavoittuvuuksia, arvioi vaikutuksia ja tarvittavia toimenpiteitä. Toimintaa ei ole ohjeistettu. Vastuuhenkilöitä ei kouluteta kyberuhkien tunnistamiseen.	41 %
Kyber- ja tietoturvariskien hallintaprosessi (tunnistus, arviointi, toimenpiteet) on ohjeistettu ja tehtävät on vastuutettu. Järjestelmien uhkien ja haavoittuvuuksien tunnistamista, vaikutusten arviointia sekä toimenpiteiden vaikuttavuutta kehitetään. Organisaation tietohallinto (tai vastaava) saa jatkuvasti mm. Kyberturvallisuuskeskukselta tietoa kyberriskeistä.	42 %
Kyber- ja tietoturvariskien hallintaprosessia (tunnistus, arviointi, toimenpiteet) käydään läpi säännöllisesti. Järjestelmien uhkien ja haavoittuvuuksien tunnistamisessa ja vaikutusten arvioimisessa sekä toimenpiteiden vaikuttavuuden parantamisessa hyödynnetään ulkopuolisia osaajia. Toteutuneet uhkatilanteet ohjaavat osaltaan tunnistamisen menettelyjen tarkastamista. Tulosen perusteella kehitetään uhkien tunnistamisen prosessia ja ohjetta.	10 %
Kyber- ja tietoturvariskien hallintaprosessi (tunnistus, arviointi, toimenpiteet) on jatkuvan parantamisen kohde. Toimintaprosessia ja ohjetta arvioidaan vuosittain. Menettelyjä kehitetään tulosten perusteella.	5 %

5. Yhteistoiminta kyber- ja tietoturvariskien hallinnassa

Organisaatio näkee kyber- ja tietoturvariskien hallintaprosessin (tunnistus, arviointi, toimenpiteet) koskevan vain organisaatiota.	0 %
Organisaation kyber- ja tietoturvariskien hallintaprosessissa (tunnistus, arviointi, toimenpiteet) yhteistoiminnan menettelytavat luodaan tapausten ilmaantuessa. Toimintaa ei ole ohjeistettu. Vastuuhenkilöitä ei kouluteta yhteistoimintaan.	32 %
Organisaation kyber- ja tietoturvariskien hallintaprosessissa (tunnistus, arviointi, toimenpiteet) yhteistyötahot on tunnistettu. Yhteistyölle on toimintaprosessi ja -ohje. Tehtävät on vastuutettu. Osapuolet välittävät toisilleen ja muille toimijoille tietoa tietoturvauhista. Organisaatio seuraa aktiivisesti viranomaisten (Kyberturvallisuuskeskus) ja laite- sekä ohjelmistotoimittajien julkaisemia haavoittuvuustiedotteita. Organisaatio on mukana yhteiskunnan kyberuhkien tunnistamisessa esimerkiksi osallistumalla harjoituksiin tai koulutustapahtumiin.	61 %
Organisaation kyber- ja tietoturvariskien hallintaprosessissa (tunnistus, arviointi, toimenpiteet) tehdään säännöllistä yhteistyötä. Tarkastusten perusteella kehitetään yhteistoimintaa.	5 %
Yhteistoiminta on jatkuvan parantamisen kohde. Toimintaprosessia ja ohjetta arvioidaan vuosittain. Menettelyjä kehitetään tulosten perusteella.	2 %

6. Yhteistoiminta

Tietoverkon hyökkäystilanteiden varalle ei ole tarvittavien osapuolten kanssa sovittua toimintatapaa.	10 %
Häiriötilanteessa tarvittavien osapuolten (organisaation sisäiset resurssit, asiakkaat, viranomaiset, laite- ja ohjelmistotoimittajat sekä asiantuntijapalveluita tarjoavat organisaatiot) välistä yhteistoimintaa ei ole ohjeistettu. Osapuolten vastuuhenkilöt on tunnistettu. Yhteistoimintamalli on keskusteltu kunkin osapuolen kanssa. Toiminta keskittyy ICT-järjestelmien hallintaan.	54 %
Häiriötilanteita varten on kuvattu yhteistoimintamalli (organisaation sisäiset resurssit, asiakkaat, viranomaiset, laite- ja ohjelmistotoimittajat sekä asiantuntijapalveluita tarjoavat organisaatiot) ja siitä on sovittu kunkin osapuolen kanssa. Yhteistyötahot on velvoitettu vastuuttamaan ja ohjeistamaan vastuuhenkilönsä toimimaan tilanteessa. Häiriötilanteessa yhteistyötahot toimivat aktiivisesti ohjeittensa mukaan. Yhteistoimintamallit kattavat ICT-järjestelmien lisäksi tuotannon ja tuotannonohjauksen mm. prosessinohjauslaitteet ja järjestelmät. Tilanteen selvittämiseksi on riittävästi päteviä henkilöitä. Vastaava häiriö pyritään jatkossa ehkäisemään.	27 %
Yhteistyötahojen kanssa harjoitellaan säännöllisesti häiriötilanteen johtamista, häiriön aikaista toimintaa, tilannetiedon muodostamista ja sen raportointia. Häiriötilanteen johtamista ja osapuolten ohjeita ja toimintatapoja kehitetään harjoitusten perusteella. Tulokset ja jatkotoimenpidesuositukset raportoidaan ylimmälle johdolle. Häiriön aikaansaanut syy pyritään poistamaan välittömästi.	7 %
Yhteistoiminta eri osapuolten kanssa häiriötilanteessa on jatkuvan parantamisen kohde. Häiriötilanteen hallinnan toimintamallia arvioidaan välittömästi tapahtuneiden tilanteiden jälkeen ja vähintään vuosittain. Häiriön hallintaa kehitetään systemaattisesti tulosten perusteella.	0 %

7. Tiedottaminen tietoturvaloukkauksista: sidosryhmät (muut kuin viranomaiset)

Tietoturvaloukkausten tiedottamisesta asiakkaille ja kumppaneille ei ole toimintatapaa.	5 %
Asiakkaiden ja kumppaneiden tiedottaminen tietoturvaloukkaustilanteessa sovitaan tapauskohtaisesti. Asianomaisille, joiden henkilötiedot voivat olla vaarantuneet, ilmoitetaan. Tiedottamisessa varaudutaan aiheeseen liittyviin lainsäädännöllisiin ja muihin pakottaviin velvoitteisiin (esim. EU:n tietosuoja-asetus). Toimintaa ei ole ohjeistettu. Vastuuhenkilöitä ei kouluteta toimimaan tilanteissa.	59 %
Organisaatiolla on prosessi ja ohje tiedottamisesta asiakkaille ja kumppaneille tietoturvaloukkauksista. Tiedottamisen tehtävät on vastuutettu. Tiedottaminen huomioi sisäisen ja ulkoisen tiedottamisen kohderyhmät (asiakkaat, kumppanit, media). Asianomaisille, joiden henkilötiedot voivat olla vaarantuneet, ilmoitetaan tapahtuneesta mahdollisimman nopeasti. Organisaatio kertoo asianosaisille, mitä palveluissa on vaarantunut, milloin palvelut on palautettu ennalleen ja miten vastaavalta vältytään jatkossa. Vastaanottajien yhteystiedot on dokumentoitu ja ajantasaiset. Erityyppisille tilanteille on valmiita tiedotepohjia. Tiedottamisprosessin ja tiedotepohjien sekä tiedotteiden vastaanottajien yhteystietojen ylläpito on vastuutettu.	32 %
Tietoturvaloukkauksien tiedottamisesta vastaavat harjoittelevat viestintää säännöllisesti. Harjoitusten tulosten perusteella kehitetään tiedottamisen menettelyjä.	3 %
Tietoturvaloukkauksista tiedottaminen on jatkuvan parantamisen kohde. Tiedottamisen menettelyjä ja -ohjeita arvioidaan vuosittain. Menettelyjä kehitetään tulosten perusteella.	7 %

8. Ilmoittaminen tietoturvaloukkauksista: muut viranomaiset

Tietoturvaloukkausten ilmoittamisesta viranomaisille ei ole toimintatapaa.	0 %
Tietoturvaloukkaustilanteessa sovitaan sen ilmoittamisesta viranomaiselle tapauskohtaisesti. Ilmoittamisessa varaudutaan aiheeseen liittyviin lainsäädännöllisiin ja muihin pakottaviin velvoitteisiin (esim. EU:n tietosuoja-asetus). Toimintaa ei ole ohjeistettu. Vastuuhenkilöitä ei kouluteta toimimaan tilanteissa.	66 %
Organisaatiolla on prosessi ja ohje ilmoittamisesta tietoturvaloukkauksista viranomaisille. Tehtävät on vastuutettu. Organisaatio kertoo viranomaisille tarkemmin havainnoistaan sekä sen, miten tapahtumaketju eteni (jotta vastaavien toistaminen maassa olisi jatkossa mahdotonta). Viranomaisten yhteystiedot on dokumentoitu ja ajantasaiset. Ilmoittamisprosessin ja yhteystietojen ylläpito on vastuutettu.	29 %
Tietoturvaloukkauksien ilmoittamisesta vastaavat harjoittelevat viestintää säännöllisesti. Harjoitusten tulosten perusteella kehitetään ilmoittamisen menettelyjä.	2 %
Tietoturvaloukkauksista ilmoittaminen on jatkuvan parantamisen kohde. Ilmoittamisen menettelyjä ja ohjeita arvioidaan vuosittain. Menettelyjä kehitetään tulosten perusteella.	3 %

Edellä olevasta taulukosta ilmenee, että useimmissa mittareista tavallisin vastaajien kypsyystaso on 2 asteikolla 1–5 (5 paras). Keskimäärin kehittämisessä ollaan pisimmällä **5** Yhteistoiminta kyber- ja tietoturvariskien hallinnassa, jossa suurin osa ilmoittaa olevansa tasolla 3 (61 prosenttia vastaajista). Näiden jälkeen seuraavaksi parhaiten on edennyt **3. ICT-varautuminen**, jossa samoin tasolla 3 on 46 prosenttia vastaajista. Kaikissa muissa mittareissa tavallisin vastaus sijoittuu kypsyystasolle 2.

Tällainen seuranta oli kyselyssä mukana nyt toista kertaa, ja sitä on tarkoitus käyttää ja kehittää palautteen pohjalta. Tulokset on raportoitu erikseen Turvallisuuskomitealle, ja niitä on esitelty Kyberkatselmus 2016 -tilaisuudessa.

LIITTEET

Liite 1 Poimintoja VAHTIn asettamispäätöksestä

Toimikausi 1.1.2015–31.12.2016

Tieto- ja kyberturvallisuuden johtoryhmän tavoitteet

VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä julkisen hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa. VAHTIn tavoitteena on tieto- ja kyberturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tavoitteena on lisäksi edistää tieto- ja kyberturvallisuuden sekä ICT-varautumisen saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista, tulosohjausta sekä tietojärjestelmien, tietoverkkojen ja tieto- ja viestintäteknisten palvelujen kehittämistä, ylläpitoa ja käyttöä. VAHTI edistää Hallitusohjelman, Yhteiskunnan turvallisuusstrategian, Suomen kyberturvallisuusstrategian, Julkisen hallinnon ICT-strategian, valtionhallinnon tietoturvallisuutta koskevan valtioneuvoston periaatepäätöksen ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä julkisen hallinnon ja erityisesti valtionhallinnon tieto- ja kyberturvallisuutta ja näihin liittyvää yhteistyötä.

Tehtävä

VAHTI on julkisen hallinnon tietoturvallisuuden kehittämisen, ohjauksen ja yhteistyön elin. VAHTI käsittelee julkisen hallinnon tieto- ja kyberturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tieto- ja kyberturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI edistää verkostomaisen toimintatavan kehittämistä julkisen hallinnon tietoturvatyössä.

Lisäksi VAHTI

- valmistelee ja sovittaa yhteen valtioneuvoston ja valtiovarainministeriön linjauksia julkisen hallinnon tieto- ja kyberturvallisuudesta ja ICT-varautumisesta sekä seuraa ja edistää niiden toimeenpanoa.
- kehittää, sovittaa yhteen ja ylläpitää julkisen hallinnon tieto- ja kyberturvallisuuden tavoitteita, toiminta-, organisointi-, arkkitehtuuri- ja resurssilinjauksia sekä normeja, ohjeita ja suosituksia.
- edistää julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta.
- käsittelee ja sovittaa yhteen julkisen hallinnon kansainvälisen tietoturvayhteistyön linjauksia ja vaikuttamista kansainvälisessä tietoturvatyössä.

- ohjaa ja käsittelee julkisen hallinnon ICT-strategiaa sekä sen valmistelua ja toimeenpanoa tieto- ja kyberturvallisuuden ja ICT-varautumisen osalta.
- ohjaa, valmistelee ja sovittaa yhteen julkisen hallinnon tieto- ja kyberturvallisuuteen liittyviä kehittämisohjelmia ja niiden toimeenpanoa.

Liite 2 Voimassa olevat VAHTI–julkaisut 31.12.2015

VAHTI 2/2015	Ohje salauskäytännöistä
VAHTI 2/2014	Tietoturvallisuuden arviointiohje
VAHTI 5/2013	Päätelaitteiden tietoturvaohje
VAHTI 4/2013	Henkilöstön tietoturvaohje
VAHTI 4b/2013	Personnel Information Security Instructions
VAHTI 1/2013	Sovelluskehityksen tietoturvaohje
VAHTI 3/2012	Teknisen ICT-ympäristön tietoturvataso-ohje
VAHTI 2/2012	ICT-varautumisen vaatimukset
VAHTI 2b/2012	Requirements for ICT Contingency Planning
VAHTI 3/2011	Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011	Johdon tietoturvaopas
VAHTI 4/2010	Sosiaalisen median tietoturvaohje
VAHTI 3/2010	Sisäverkko-ohje
VAHTI 2/2010	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 2b/2010	Instructions on Implementing the Decree on Information Security in Central Government
VAHTI 2c/2010	Anvisning om verkställighet av förordningen om informationssäkerheten inom statsförvaltningen
VAHTI 7/2009	Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009	Kohdistetut hyökkäykset (uudistettavana)
VAHTI 5/2009	Effective Information Security
VAHTI 3/2009	Lokiohje
VAHTI 2/2009	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin (uudistettavana)
VAHTI 9/2008	Hankkeen tietoturvaohje
VAHTI 8/2008	Valtionhallinnon tietoturvasanasto
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen (uudistettavana)
VAHTI 6/2008	Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista
VAHTI 5/2008	Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys
VAHTI 4/2008	Valtionhallinnon tietoturva-arviointipoolin toimintaraportti
VAHTI 3/2008	Valtionhallinnon salauskäytäntöjen tietoturvaohje (uudistettavana)
VAHTI 2/2008	Tärkein tekijä on ihminen – Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007	Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 1/2007	Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä

VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa (uudistettavana)
VAHTI 11/2006	Tietoturvakouluttajan opas
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 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 3/2005	Tietoturvapoikkeamatilanteiden hallinta (uudistettavana)
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (uudistettavana)
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje (uudistettavana)
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002	Valtionhallinnon etätyön tietoturvaohje
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje (uudistettavana)

Ohjeisto löytyy VAHTIn Internet-sivuilta http://www.vahtiohje.fi/

Liite 3 VAHTI-hankkeet 2015

Toiminnan organisointi	Vetäjä	Organisaatio
Valtion tietoturvallisuuden johtoryhmä VAHTI	Mikael Kiviniemi /	VM
	Aku Hilve	VM
VAHTI sihteeristö	Aku Hilve /	VM
	Kimmo Rousku	Valtori / VM
VAHTI tekninen jaosto	Kimmo Rousku	Valtori / VM
VAHTI ohjejaosto	Pekka Ristimäki	VRK
VAHTI kuntajaosto	Harri Ihalainen	Rovaniemen kaupunki
Hankkeet		
1. VAHTI ohjeiden ruotsinnokset (M)	Ralf Sontag	Huoltovarmuuskeskus
2. VAHTI ohjeiden englanniksi kääntäminen (M)	Tuire Saaripuu	Väestörekisterikeskus
3. Korotetun tietoturvatason ja ICT -varautumisen yhteishanke (M)	Hanna Heikkinen	Valtori
4. Tietoturvapoikkeamien hallinta (M)	Juha Ilkka	VNK
5. Toiminnan jatkuvuuden hallinta (M)	Riitta Gröhn	Aalto-yliopisto
6. Sähköisen asioinnin tietoturvallisuus (M)	Kimmo Janhunen	Oikeusrekisterikeskus
7. VAHTI-rakennehanke (M)	Kirsi Janhunen	VM
VAHTIn seurannassa olevat hankkeet		
8. Valtion ympärivuorokautisen tietoturva-toiminnan kehittämishanke (SecICT) (M)	Kirsi Janhunen	VM

Taulukossa on (V) tarkoittaa valmistunutta hanketta ja (M) meneillään olevaa hanketta.

Hankkeiden toiminta vuonna 2015

Tässä liitteessä kuvataan tiiviisti VAHTI-hankkeiden toimintaa vuonna 2015. Kuvaukseen ei sisälly VAHTIn muun kehitys-, ohjaus ja yhteistyön selostamista eikä JulkICT:n hankkeita.

VAHTIn tekninen jaosto (VM047:18/2007)

Tavoitteet
Jaoston tavoitteena on edesauttaa valtionhallinnossa käytössä olevien tietoturvavaatimusten hyödyntämistä sekä kehittää näiden vaatimusten oikeaoppista käyttöä ja tulkintaa. Samoin tavoitteena on tietoturvavaatimuksia koskevan osaamisen kasvattaminen valtionhallinnon organisaatioiden kaikilla tasoilla.

Teknisen jaoston tehtävänä on tehdä linjauksia ja ohjeistaa tekniseen tietoturvallisuuteen liittyvissä kysymyksissä. Tehtäviensä hoitamiseksi teknisen jaoston tulee mm.

- tulkita kansallisia tietoturvavelvoitteita koskevien tietoturvavaatimuksien ja -kriteeristöjen teknisten tietoturvavaatimusten toimeenpanoa.
- tuottaa tulkintojen perusteella teknisen infrastruktuurin, sovellushankkeiden ja hankintojen tueksi esimerkkiratkaisuja ja mahdollisuuksien mukaan yleisimpiä tulkintoja. Kattavien yleistulkintojen teko teknisistä tietojenkäsittely-ympäristöistä ei katsota olevan mahdollista, joten malliratkaisut nähdään tässä toimivana menettelytapana.
- toimia asiantuntijaryhmänä VAHTIn sekä keskeisten hankkeiden tarpeissa, ja
- tukea tietoturvavaatimusten ja -kriteeristöjen huomioimista.
- edustaa tieto- ja kyberturvallisuuden näkökulmaa valtionhallinnon keskeisten ICT-hankintojen asiantuntijatukiryhmänä. Ryhmälle tuodaan käsiteltäväksi ja kommentoitavaksi käytettävien tietoturvavaatimusten näkökulmasta kaikki valtionhallinnon keskeiset yhteiset tai hallinnonalojen merkittävät ICT-kilpailutukset.

Toteutus
Hanke toteutetaan työryhmämuotoisena työskentelynä, jonka toiminnasta vastaavat puheenjohtaja, varapuheenjohtaja sekä sihteeri. Jaostossa on laaja-alainen edustus ja osaaminen keskeisistä valtionhallinnon teknistä tietoturvallisuutta ja hankintoja toteuttavista organisaatioista. Jaosto kokoontui seitsemän kertaa vuonna 2015.

Tulokset
Vuoden 2015 aikana on julkaistu:

- VAHTI 2/2015 Ohje salauskäytännöistä sekä pidetty sen jalkautusseminaari valtionhallinnolle, käynnistetty vastaavanlaisen tilaisuuden suunnittelu ICT-palvelutoimittajille alkuvuodelle 2016.

Tämän ohella toteutettiin ICT-hankintojen tietoturvaseminaari 12.5.2015 sekä julkaistiin tätä tukeva tukimateriaali 12 Liite 5. Tietoturvallisuuden ja jatkuvuudenhallinnan huomioiminen hankittaessa ulkoistettuja ICT-palveluita. Lisäksi julkaistiin VAHTI 4/2013 Henkilöstön tietoturvaohjeen uusi tukimateriaali; – 9. Liite 6 tietoturvallisuuden huomioiminen ulkomaille matkustettaessa tai siellä työskenneltäessä.

Vaikuttavuus
Tekninen jaosto on tuottamiensa materiaalien, tekemiensä kyselyiden ja linjausten avulla pystynyt parantamaan valtionhallinnon tietoutta sen omasta tietoturvallisuuden tilasta sekä luomaan teknisen tietoturvallisuuden tilannekuvaa sekä uusimaan tiedon salaukseen liittyvää ohjeistusta. Niiden avulla on voitu parantaa myös valtionhallinnon palveluiden tietoturvallisuutta.

VAHTI ohjejaosto (VM136:05/2013)

Tavoitteet
Vahti ohjejaoston tavoitteet ovat:

- VAHTI-ohjeistus on sisällöltään ajantasainen
- VAHTI-ohjeistuksen päivitysvastuut ja -prosessi ovat selkeät
- VAHTI-ohjeistuksen rakenne ja julkaisukanavat tukevat ja mahdollistavat helpon tiedon saatavuuden ja käytön.

Toteutus
Vuonna 2015 ohjejaoston toiminnan painopiste oli asettamispäätöksen mukaisesti VAHTI-ohjeiden sisällön uudistaminen. Tämän johdosta ohjejaosto käynnisti kolme ohjehanketta:

- Sähköisen asioinnin tietoturvallisuus, toimikausi 6.5.2015–31.5.2016
- Tietoturvapoikkeamien hallinta, toimikausi 6.5.2015–31.5.2016
- Toiminnan jatkuvuuden varmistaminen, toimikausi 6.5.2015–31.12.2016.

Ohjejaosto valmisteli pääosin syksyn 2015 aikana VAHTI-ohjeistuksen rakenteen, sisällön ja näitä tukevan sähköisen julkaisukanavan tavoitetilaa. Tämän valmistelun pohjalta VAHTI johtoryhmä asetti joulukuussa 2015 VAHTIn tieto- ja kyberturvallisuuden hallintarakenteen päivittämisen hankeryhmän. Tämän kehityshankkeen toimikausi on 8.12.2015–31.12.2016. Hankkeen tehtävänä on selkiyttää julkishallinnon tieto- ja kyberturvallisuuden vaatimuksia ja niiden velvoittavuutta. Tämä tapahtuu luomalla asiakaslähtöinen selkeä rakenne, missä yhteydessä päivitetään olemassa oleva VAHTI-ohjeistus viemällä se soveltuvin osin uuteen hallintarakenteeseen.

Uudistuksen keskeiset tavoitteet ovat:

- rakenteen, vaatimusten ja ohjeistuksen selkiyttäminen sekä yksinkertaistaminen
- päällekkäisyyksien poistaminen
- ylläpidettävyyden helpottaminen
- käyttäjien tarpeiden ja käytettävyyden parempi huomioon ottaminen
- auditointien ja tarkastusten selkiyttäminen
- kustannustehokkuuden lisääminen
- sähköisen julkaisukanavan toteuttaminen.

Toukokuussa 2015 käynnistettiin valtionhallinnon turvallisuussopimusmallin päivitystyö, jonka valmistelusta vastaa pääosin Hansel. Uusi turvallisuussopimusmalli julkistetaan keväällä 2016. Työssä on huomioitu uusi turvallisuusselvityslaki, VAHTI-suositukset (toimitilojen tietoturvaohje), Teknisen jaoston lausunto (Toimittajan sisäinen tietojenkäsittely), Katakri III sekä muut käytössä olleet turvallisuussopimusmallit. Sopimusmallin sisältöä pyritään myös selkeyttämään.

Tulokset
Vuoden aikana käynnistettiin neljä hanketta, jotka ovat toimineet aktiivisesti. Päivitetty turvallisuussopimusmalli oli lausuntokierroksella valtionhallinnossa.

Vaikuttavuus
VAHTI-ohjeet ovat laajasti käytössä valtionhallinnossa ja sen ulkopuolella. Ne tukevat vaatimustenmukaisuuden täyttymistä sekä hyvien tietoturvakäytänteiden toteuttamista. VAHTI-ohjejaoston toiminta tulee nopeuttamaan ohjeiden laatimisprosessia, varmistamaan ohjeistuksen tasalaatuisuutta sekä kehitettävien jakelukanavien myötä palvelemaan paremmin ohjeistusta käyttävien tahojen tietotarpeita.

VAHTI kuntajaosto (VM136:06/2013)

Tavoitteet
Kuntien tietoturvajaosto tukee toiminnallaan valtiovarainministeriötä, VAHTIa sekä kuntia tieto- ja kyberturvallisuuteen liittyvässä kehittämisessä ja sen valmistelussa. Jaoston yleisenä tavoitteena on tieto- ja kyberturvallisuutta ja siihen liittyvää yhteistyötä kehittämällä parantaa kuntien toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista.

Toteutus
Hanke toteutetaan ohjausryhmään kuuluvien henkilöiden tekemänä. Ryhmään kuuluu valtiovarainministeriön sekä useiden kuntien ja kuntayhtymien edustajat. Työ toteutetaan ennakkovalmisteltuina ryhmäkokouksina.

Tulokset
Jaosto valmisteli kunnille suunnatun tieto- ja kyberturvallisuuskyselyn, joka lähetettiin kuntien kirjaamoihin kesälomien jälkeen. Kyselyyn vastasi 93 kuntaa, joille lähetettiin koosteraportti oman kunnan tilasta suhteessa kuntien keskiarvoon.

Marraskuussa jaosto järjesti kuntajohdolle suunnatun tieto- ja kyberturvallisuus seminaarin Helsingissä. Tilaisuuden tavoitteena oli selventää kuntajohdolle, mitä tieto- ja kyberturvallisuus tarkoittaa kuntajohtamisen arjessa. Lisäksi tilaisuudessa esiteltiin kuntakyselyn raportit ja niihin liittyvät jatkotoimet.

Jaosto on toiminut tiiviissä yhteistyössä tietosuojavaltuutetun toimiston kanssa ja ottanut toiminnassaan huomioon hallitusohjelman, kuntalain ja sen kehittämisen sekä EU:n uuden tietosuoja-asetuksen.

Vaikuttavuus
Kuntien tietoturvatyön vahvistamisella ja tietoturvatietoisuuden lisäämisellä on suuri vaikutus kunnallisten palveluiden turvallisuuteen sekä kansalaisten luottamuksen lisäämiseen palveluita kohtaan.

VAHTI-ohjeiden ruotsinnosten ohjausryhmä (VM036:02/2013)

Ryhmällä ei ollut toimintaa vuonna 2015.

VAHTI-ohjeiden englanniksi kääntämisen ohjausryhmä (VM036:03/2013)

Ryhmällä ei ollut toimintaa vuonna 2015.

Korotetun tietoturvatason ja ICT -varautumisen yhteishanke, KoTVa (VM136:04/2013)

Tavoitteet
Hankkeen tavoitteena on, että kukin osallistuva organisaatio saavuttaa hankkeeseen valitussa suojattavassa kohteessa tietoturvallisuuden korotetun tason sekä asetetun ICT-varautumisen tason. Se syventää aiemmissa yhteishankkeissa käsiteltyjä tietoturvallisuuden hallinnan hyviä käytäntöjä erityisesti suojattavien kohteiden turvaamisen näkökulmasta. Tavoitteena on, että valtionhallinnon organisaatioilla on menettelyt, joilla ne kykenevät tunnistamaan toimintansa suojattavat kohteet, arvioimaan niihin kohdistuvat riskit, määrittämään niissä käsiteltävien tietojen suojaustasot ja niissä käytettävien järjestelmien kriittisyys- ja varautumistasot sekä valitsemaan ja asettamaan tarvittavat turvakontrollit, huomioiden myös kyberturvallisuusstrategian toimeenpano-ohjelman.

Toteutus
Hankkeen järjestävä taho neuvoo ja opastaa vaatimusten eri toteutustavoissa. Hankkeeseen osallistuva organisaatio saa käyttöönsä materiaalin ja työkalut korotetun tietoturvaja asetetun varautumisen tason toteuttamiseen sekä näihin tarvittavan koulutuksen. Osallistujat saavat toisiltaan hyödyllisiä käytännön neuvoja eri vaatimusten mahdollisista toteutustavoista. Suojattavissa kohteissa keskitytään erityisesti ICT-ympäristöihin ja niiden keskeisimpiin turvakontrolleihin. Hankkeessa on toteutettu vuonna 2015 työpajoja ja muita tilaisuuksia ryhmätöineen ja kotitehtävineen yhteensä yhdeksän kertaa.

Tulokset
Hankkeen keskeisin lopputulos on, että osallistuvan organisaation ja valitun kohteen tietoturvallisuuden sekä jatkuvuudenhallinnan taso paranee. Hanke luo osallistuvalle organisaatiolle keinot valitun järjestelmän tietoturvallisuuden hallinnan ohjaamiseksi ja ylläpitämiseksi.

Vaikuttavuus
Organisaatio voi käyttää hankkeen aikana kertynyttä oppia ja materiaalia muiden korotettua tasoa vaativien palvelujen, toimintojen ja tietojärjestelmien kehitystyöhön. Hankkeen kautta saatua osaamista ja malleja voidaan hyödyntää myös muualla valtionhallinnossa. Hanke edistää myös Suomen kyberturvallisuusstrategian tavoitteiden saavuttamista.

Tietoturvapoikkeamien hallinta (VM136:09/2013)

Tavoitteet
Tietoturvapoikkeamaryhmän tavoitteena on parantaa tietoteknisten järjestelmien ja verkkojen sekä palvelujen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista kehittämällä tietoturvapoikkeamien hallintaa. Tavoitteena on lisäksi vahvistaa tietoturvapoikkeamien hallinnan hyviä käytäntöjä.

Toteutus
Ohjeuudistuksessa on huomioitu tietoturvallisuuden yleinen kehitys sekä kohdistettujen hyökkäysten kasvu ja ammattimaistuminen viime vuosina. Uuteen ohjeeseen tullaan sisällyttämään kansalliset ja kansainväliset vaatimukset sekä yleisimpien viitekehysten ja standardien parhaat käytännöt poikkeamienhallintatyölle.

Tulokset
Työryhmä on käynnistänyt tietoturvapoikkeamien hallintaa koskevien VAHTI-ohjeiden päivitystyön, joka tullaan saattamaan päätökseen kevään 2016 aikana.

Vaikuttavuus
Ohjetta tullaan hyödyntämään valtionhallinnon lisäksi myös muualla julkishallinnossa ja yksityisellä sektorilla.

Toiminnan jatkuvuuden hallinta (VM136:08/2013)

Tavoitteet
Hankkeen tavoitteena on jatkuvuuden hallintaa ja ICT-varautumista kehittämällä parantaa toimintojen, tietojärjestelmien ja verkkojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Lisäksi tavoitteena on edistää jatkuvuuden ja ICT-varautumisen saattamista kiinteäksi osaksi julkisen hallinnon toimintaa, johtamista ja palveluita.

Toteutus
Painopisteeksi määriteltiin jatkuvuuden hallintaa ja ICT-varautumista koskevien ohjeiden uudistaminen ja yhtenäistäminen. Hankkeessa on laadittu uusi menettelytapaohje jatkuvuuden hallinnan toteuttamisesta julkishallinnon organisaatioissa. Työryhmä ei kuitenkaan lähtenyt korvaamaan olemassa olevia ICT-varautumisen vaatimuksia, vaan niiden arviointi sisällytetään laajempaan vaatimusten uudistamistyöhön.

Tulokset
Työryhmä on laatinut Jatkuvuuden hallinnan turvaamisesta ohjeluonnoksen, jonka valtiovarainministeriö lähetti lausuntokierrokselle helmikuussa 2016.

Vaikuttavuus
Ohjeessa kuvattujen menettelyiden käyttöönotto tulee parantamaan merkittävästi varautumista erilaisiin häiriö- ja poikkeamatilanteisiin sekä mahdollistaa niistä nopeamman toipumisen ja paluun normaalitoimintaan.

Sähköisen asioinnin tietoturvallisuus (VM136:07/2013)

Tavoitteet
Hankeryhmän tehtävänä on yhdistää ja päivittää sähköisen asioinnin ja palveluiden tietoturvallisuuteen ja tunnistamiseen julkishallinnon verkkopalveluihin liittyvät VAHTI-ohjeet. Hankeryhmän yleisenä tavoitteena on sähköisen asioinnin tietoturvallisuutta kehittämällä parantaa sähköisten palveluiden luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tavoitteena on lisäksi vahvistaa tieto- ja kyberturvallisuuden sekä ICT-varautumisen saattamista kiinteäksi osaksi sähköisten palveluiden kehittämistä, ylläpitoa ja käyttöä.

Toteutus
Hanke toteutetaan hankeryhmään kuuluvien henkilöiden tekemänä virkatyönä ja ulkopuolisen konsultin (asiantuntijasihteerin) yhdistelmänä. Hankeryhmään kuuluu edustajia useista julkishallinnon organisaatioista. Hankeryhmä kartoittaa eri organisaatioiden sähköisen asioinnin ratkaisuja ja niiden tietoturvallisuutta sekä pyytää ulkopuolisia asiantuntijoita esittelemään sähköiseen asioinnin tietoturvallisuuden ja sähköisen asioinnin viitearkkitehtuuriin hankkeitaan. Erityisesti kansallisen palveluarkkitehtuurin hankkeen tuottamat tukipalvelut huomioidaan ohjeen sisällössä. Hankeryhmä kokoontui vuonna 2015 kolme kertaa.

Tulokset
Ei tuloksia vuonna 2015.

Vaikuttavuus
Ei vaikuttavuutta vielä vuonna 2015. Organisaatiot voivat odottaa sähköisen asioinnin palveluiden tietoturvallisuuden suunnitteluun ja huomioimiseen apuja ohjeen ja laadittavan viitearkkitehtuurin valmistuessa vuonna 2016.

Valtion ympärivuorokautisen tietoturvatoiminnan kehittämishanke, SecICT (VM018:00/2013)

Tavoitteet
SecICT-hankkeen tavoitteena on parantaa valtion kykyä ennaltaehkäistä ja hoitaa vakavia sekä laajavaikutteisia tieto- ja kyberhäiriötilanteita.

Toteutus
Hankkeen omistaa JulkICT, VAHTI toimii hankkeen seurantaryhmänä. Hanke käynnistyi vuonna 2013 ja se valmistuu vuoden 2016 aikana. Vuoden 2015 keskeisenä painopisteenä on valtion yhteisen tieto- ja kyberturvallisuuden tilannekuvaympäristön suunnittelu, laajavaikutteisten tieto- ja kyberhäiriötilanteiden hallintaan tarvittavan toimijaverkoston kokoaminen ja viranomaisten häiriönhallintayhteistyön kehittäminen (VIRT-toiminta). Viranomaiset tekevät hankkeessa laajaa yhteistyötä.

Tulokset
Hankkeessa on vuoden 2015 loppuun mennessä:

- laajennettu Viestintäviraston CERT-palvelut GovCERT- ja GovHAVARO-palveluina valtionhallintoon,
- pilotoitu Huoltovarmuuskeskuksen HUOVI-palvelua valtionhallintoon,
- luotu osa tieto- ja kyberhäiriöiden hallinnan toimijaverkostosta,
- perustettu viranomaisten häiriönhallintayhteistyötoiminnan elin (VIRT-toiminta).

Lisäksi hankkeessa on kehitetty häiriönhallintakonsepti tukemaan Valtorin tietoturvapoikkeamien hallintaa. Hankkeen tuloksia on käsitelty VAHTI-johtoryhmässä vuoden 2015 aikana.

Vaikuttavuus
SecICT-hanke on keskeinen kansallista tieto- ja kyberturvallisuutta kehittävä sekä kyberturvallisuusstrategian toimeenpano-ohjelman useaa osa-aluetta toteuttava hanke. Hankkeen tuloksena saadaan tehokkaampi yhteistoiminta viranomaisten ja häiriötilanteiden kohteena olevien kesken, sekä parempi varautuminen vakaviin ja laajavaikutteisiin häiriötilanteisiin. Keskitetyn tieto- ja kyberturvallisuuden tilannekuvan avulla varmistetaan, että tarvittavilla osapuolilla on oikea ja oikea-aikainen tieto käytettävissä päätöksentekoon, toimenpiteisiin sekä viestintään. Hankkeessa kehitettävän VIRT-toiminnan kautta eri toimijoiden roolit häiriötilanteissa selkeytyvät.

Hanke tukee myös analysointikyvyn ja toimijaverkoston kehittämisen kautta valtiovarainministeriön kyvykkyyttä määrätä poikkeusoloissa valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä valmiuslain 105 §:n mukaisesti.

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
Telefaksi 09 160 33123
www.vm.fi

ISSN 1798-0860 (pdf)
ISBN 978-952-251-760-9 (pdf)

Toukokuu 2016